

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年9月30日 (30.09.2004)

PCT

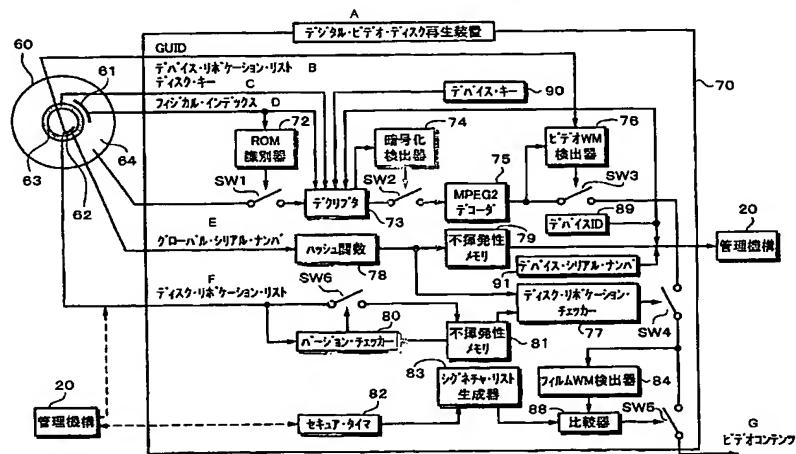
(10) 国際公開番号
WO 2004/084208 A1

- (51) 国際特許分類: G11B 20/10, 20/12, 7/005, H04N 5/91, G06F 12/14
- (21) 国際出願番号: PCT/JP2004/003077
- (22) 国際出願日: 2004年3月10日 (10.03.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2003-078375 2003年3月20日 (20.03.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP). ソニー ピクチャーズ エンターテイメント (SONY PICTURES ENTERTAINMENT) [US/US]; 90232 カリフォルニア州カルバーシティウエストワシントンブルーバード 10202 California (US).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI, Satoshi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). エクランド・チャールズ・ドン (EKLUND, Charles Don) [US/US]; 90232 カリフォルニア州カルバーシティウエストワシントンブルーバード 10202 ソニー ピクチャーズ エンターテイメント内 California (US). 佐藤 英雄 (SATO, Hideo) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 米満 潤 (YONEMITSU, Jun) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU, Katsumi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 杉浦 正知, 外 (SUGIURA, Masatomo et al.); 〒1710022 東京都豊島区南池袋2丁目49番7号 池袋パークビル7階 Tokyo (JP).

[続葉有]

(54) Title: RECORDING MEDIUM, MANUFACTURING METHOD THEREOF, REPRODUCTION METHOD, REPRODUCTION DEVICE, AND COPYRIGHT MANAGEMENT METHOD

(54) 発明の名称: 記録媒体及びその製造方法、再生方法及び再生装置、並びに著作権管理方法



- A...DIGITAL VIDEO DISC REPRODUCTION DEVICE
B...DEVICE REVOCATION LIST
C...DISC KEY
D...PHYSICAL INDEX
90...DEVICE KEY
72...ROM IDENTIFIER
E...GLOBAL SERIAL NUMBER
F...DISC REVOCATION LIST
20...MANAGEMENT MECHANISM
74...ENCRYPTION DETECTOR
73...DECRYPTER
78...HASH FUNCTION
80...VERSION CHECKER
82...SECURE TIMER
75...MPEG2 DECODER
76...NON-VOLATILE MEMORY
81...NON-VOLATILE MEMORY
83...SIGNATURE LIST GENERATOR
76...VIDEO WM DETECTOR
89...DEVICE ID
91...DEVICE SERIAL NUMBER
77...DISC REVOCATION CHECKER
84...FILM WM DETECTOR
88...COMPARATOR
G...VIDEO CONTENT

(57) Abstract: A GUID as title information and a global serial number are recorded on a BCA of a digital video disc (60) and a Hash value of the GUID is embedded as a watermark in a data area (64). Upon reproduction, check is made whether these two GUID information coincide, thereby preventing unauthorized copying. A disc revocation list is provided from a lead in area

[続葉有]



(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL,

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(63) and a management mechanism (20). By using the global serial number and the disc revocation list, it is possible to exclude an unauthorized disc. Data embedded in a film to be screened is detected by a film WM detector (84) so as to exclude a disc containing the data. Thus, it is possible to exclude a disc distributed in an unauthorized manner before being allowed by the copyright manager.

(57) 要約: デジタル・ビデオ・ディスク60のBCAにタイトル情報であるGUIDとグローバル・シリアル・ナンバを記録し、データエリア64にGUIDのハッシュ値を電子透かしとして埋め込む。再生時に、これら2つのGUIDの情報の一致を確認することで不正コピーを排除する。リードインエリア63や管理機構20からディスク・リボケーション・リストが提供される。グローバル・シリアル・ナンバと、ディスク・リボケーション・リストにより不正なディスクを排除することができる。上映用の映画に埋め込まれたデータをフィルムWM検出器84が検出してそのデータが記録されたディスクを排除することができる。これにより、著作権管理者が許可する前に不正に流通したディスクを排除することができる。

明 細 書

記録媒体及びその製造方法、再生方法及び再生装置、並びに著作権管理方法

5

技術分野

この発明は、特に不正な複製行為による映画等のコンテンツの利用を防止する記録媒体およびその製造方法、再生方法および再生装置、並びに著作権管理方法に関する。

10

背景技術

近年開発されたDVD (Digital Versatile Disc)等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

DVD-Videoでは、コピープロテクション技術としてCSS (Content Scramble System)が採用されている。CSSは、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSSの利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのまるとコピー（ビットバイビットコピー）することは、CSS契約上では、認められた行為ではない。

25 CSSの後に、DVD-Audio等のDVD-ROMの著作権保護技術であるCPPM (Content Protection for Pre-Recorded Media)、並

びに記録型DVD、メモリカードに関する著作権保護技術CPRM (Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を
5 制限できる特徴を有している。DVDに関する著作権保護の方法に関しては、“山田, 「DVDを起点に著作権保護空間を広げる」, 日経エレクトロニクス 2001.8.13, p.143-153” に説明され、CPRMは、ライセンス管理者である米4C Entity, LLCが配布する、“Content Protection for Recordable Media Specification DVD Book”、インターネット<U
10 RL : <http://www.4Centity.com/>>に説明されている。

しかしながら、映画コンテンツの不正な複製行為が現実には発生しており、HD (High Definition) デジタルビデオカメラやHDデジタルビデオディスク記録の民生市場での実用化が見込まれる中で、この状況を解決せずに放置することは、著作権者の利益確保に深刻な影響を及ぼす
15 事態を招くことは想像に難くない。不正な複製行為の事例を以下に列挙する。

<1. 映画館での撮影・盗難>

映画館で上映される新作の映画をデジタル・ビデオ・カメラで撮影し、これをソースとしてROM化されたDVD-Videoを製造することが行
20 われている。また、映画館で上映するフィルムをその価値に見合う対価を支払うことなく、かつ権利保有の許諾を得ることなくテレシネ作業によりベースバンド・ビデオ信号へ変換し、これをソースとしてROM化された海賊版DVD-Videoを製造することが可能である。

<2. DVD-Video正規品からの複製 (「DeCSS」の利用)>

25 CSSの暗号を破るDeCSSソフトウェアがインターネット上で配布され誰でも簡単に入手でき、これを用いて暗号を解いて平文の状態で

記録型DVDへ書き込むことが可能である。このコンテンツをDVD製造工場へ持ち込むことでROM化されたDVD-Videoを製造することも可能である。

＜3. DVD-Video正規品からの複製（アナログ出力の利用）＞

- 5 パーソナルコンピュータ（以下、適宜PCと略す）は専用機器ではないことから、CGMS-A（Copy Generation Management System - Analog）やマクロビジョン信号の反応義務はなく、コピー制限は有効に働かないことから、DVD-Videoプレーヤからの出力をPC内蔵のビデオキャプチャードへ入力してHDD（Hard Disc Drive）へコピー
- 10 することが可能である。一旦HDDへ記録されたビデオ・データは平文の状態で記録型DVDへ書き込むことができる。このコンテンツをDVD製造工場へ持ち込むことでROM化されたDVD-Videoを製造することも可能である。

＜4. DVD-Video正規品からの複製（DVD製造工場での不正製造行為）＞

- 15 DVD製造工場において、受注量よりも余分にDVDを製造し、この余分を不正な流通業者へ横流しをして闇マーケットで販売することが可能である。

＜5. DVD-Video正規品からの複製（原盤への転写）＞

- 20 市販されているDVD-Videoから直接転写することで原盤を起こし、これを複製用のマスターとしてROM化されたDVD-Videoを製造することが可能である。

- このような不正な複製行為に関する問題解決に至る技術的方法の提案は、上述したCSS、CPPMおよびCPRMなどの従来の著作権保護
- 25 技術においてはなされていない。

したがって、この発明の目的は、ビデオコンテンツの不正な複製行為

から著作権者の利益を守ることができる記録媒体およびその製造方法、再生方法および再生装置、並びに著作権管理方法を提供することにある。

発明の開示

- 5 上述した課題を解決するために、請求の範囲第1項の発明は、ビデオコンテンツのデータが記録されている記録媒体であって、ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル情報の真正性の保証に必要となるタイトルメッセージが、ビデオコンテンツのデータに電子透かし情報として埋め込まれ、タイトル情報またはタイトルメッセ
- 10 ージが、データの記録されている領域と異なる記録領域に記録される記録媒体である。

- 請求の範囲第3項の発明は、ビデオコンテンツのデータが記録された記録媒体が製造される記録媒体製造方法であって、ビデオコンテンツのデータを編集する編集ステップと、ビデオコンテンツのタイトルを示す
- 15 タイトル情報または当該タイトル情報の真正性の保証に必要となるタイトルメッセージを、ビデオコンテンツのデータに電子透かし情報として埋め込む第一のタイトル記録ステップと、タイトル情報またはタイトルメッセージが、データの記録されている領域と異なる記録領域に記録される第二のタイトル記録ステップとを有する記録媒体製造方法である。

- 20 請求の範囲第6項の発明は、ビデオコンテンツのデータが記録され、当該ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル情報の真正性の保証に必要となるタイトルメッセージがビデオコンテンツのデータに電子透かし情報として埋め込まれ、タイトル情報またはタイトルメッセージがデータの記録されている領域と異なる記録領域に
- 25 記録された記録媒体を再生する再生方法であって、データの記録されている領域と異なる記録領域に記録されているタイトル情報またはタイト

ルメッセージを検出する第一のタイトル情報検出ステップと、電子透かし情報として埋め込まれているタイトル情報またはタイトルメッセージを検出する第二のタイトル情報検出ステップと、第一及び第二のタイトル情報検出ステップでそれぞれ検出されたタイトル情報またはタイトル
5 メッセージの真正性が保証されるか否かを判定する判定ステップと、判定ステップで真正性が保証されなかった場合には記録媒体の再生動作を制限する再生制限ステップとを有する再生方法である。

請求の範囲第7項の発明は、ビデオコンテンツのデータが記録され、当該ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル
10 ル情報の真正性の保証に必要なタイトルメッセージがビデオコンテンツのデータに電子透かし情報として埋め込まれ、タイトル情報またはタイトルメッセージがデータの記録されている領域と異なる記録領域に記録された記録媒体を再生する再生装置であって、データの記録されている領域と異なる記録領域に記録されているタイトル情報またはタイト
15 ルメッセージを検出する第一のタイトル情報検出部と、電子透かし情報として埋め込まれているタイトル情報またはタイトルメッセージを検出する第二のタイトル情報検出部と、第一及び第二のタイトル情報検出部でそれぞれ検出されたタイトル情報またはタイトルメッセージの真正性が保証されるか否かを判定する判定部と、判定部で真正性が保証されな
20 かった場合には記録媒体の再生動作を制限する制御部とを有する再生装置である。

請求の範囲第8項の発明は、ビデオコンテンツのデータが記録されている記録媒体であって、一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報と、リボークすべき記録媒体を、少なくとも媒体識別情
25 報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストとが記録されている記録媒体である。

請求の範囲第 14 項の発明は、ビデオコンテンツのデータが記録された記録媒体が製造される記録媒体製造方法であって、ビデオコンテンツのデータを編集する編集ステップと、リボークすべき記録媒体を、少なくとも一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストを記録する媒体リスト記録ステップと、各媒体毎の媒体識別情報がビデオコンテンツのデータが記録された領域の記録方法と異なる方法で記録する識別情報記録ステップとを有する記録媒体製造方法である。

10 請求の範囲第 20 項の発明は、ビデオコンテンツのデータが記録され、一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報と、リボークすべき記録媒体を、少なくとも媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストとが記録されている記録媒体を再生する再生方法であって、
15 媒体識別情報を読み出す媒体識別情報読み出しステップと、媒体リボケーション・リストを読み出す媒体リスト読み出しステップと、読み出した媒体識別情報または当該媒体識別情報の識別メッセージをメモリに蓄積する媒体識別情報蓄積ステップと、蓄積された媒体識別情報または識別メッセージが媒体リボケーション・リストに含まれているか否かを判定する媒体リスト判定ステップと、媒体リスト判定ステップでリボークすべきと判断された場合には記録媒体の再生動作を制限する再生制限ステップとを有する再生方法である。

請求の範囲第 25 項の発明は、ビデオコンテンツのデータが記録され、一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報が記録されている記録媒体を再生する再生方法であって、媒体識別情報を読み出す媒体識別情報読み出しステップと、読み出した媒体識別情報または当

25

- 該媒体識別情報の識別メッセージをメモリに蓄積する媒体識別情報蓄積部と、著作権管理サーバとネットワークを介して接続し、当該著作権管理サーバからリボークすべき記録媒体を前記媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボ
- 5 ケーション・リストを受信し、蓄積した媒体識別情報または当該媒体識別情報の識別メッセージが媒体リボケーション・リストに含まれているか否かを判定する媒体リスト判定ステップとを有し、判定ステップでリボークすべきと判断された場合には記録媒体の再生動作を制限する再生制限ステップとを有する再生方法である。
- 10 請求の範囲第30項の発明は、ビデオコンテンツのデータが記録されている記録媒体を再生する再生装置であって、一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報と、リボークすべき記録媒体を、少なくとも媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストとを読み出す
- 15 読み出し部と、読み出した媒体識別情報または当該媒体識別情報の識別メッセージを蓄積する媒体識別情報蓄積部と、蓄積された媒体識別情報または識別メッセージが媒体リボケーション・リストに含まれているか否かを判定する判定部と、判定部でリボークすべきと判断された場合には記録媒体の再生動作を制限する制御部とを有する再生装置である。
- 20 請求の範囲第35項の発明は、ビデオコンテンツのデータが記録されている記録媒体を再生する再生装置であって、一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報を読み出す読み出し部と、読み出した媒体識別情報または当該媒体識別情報の識別メッセージを蓄積する媒体識別情報蓄積部と、著作権管理サーバからリボークすべき記録媒体
- 25 を媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストを受信する媒体リスト

受信部と、蓄積した媒体識別情報または識別メッセージが受信した媒体リポケーション・リストに含まれているか否かを判定する媒体リスト判定部と、媒体リスト判定部でリボークすべきと判断された場合には記録媒体の再生動作を制限する制御部とを有する再生装置である。

- 5 請求の範囲第40項の発明は、複数の再生装置と著作権管理者の認可を受けた著作権管理サーバとがネットワークを介して接続されたシステムにおける著作権管理方法において、再生装置のそれぞれは、ビデオコンテンツのデータが記録され、一連の記録媒体毎に、各記録媒体を一意に識別する媒体識別情報が記録されている記録媒体を再生し、記録媒体
- 10 の媒体識別情報を読み出し、読み出した媒体識別情報から一方向性の関数により得られる識別メッセージを機器識別情報と共に著作権管理サーバに送信し、著作権管理サーバは、機器識別情報と識別メッセージとを受信し、受信データの集合から複数の再生装置における同一の記録媒体の再生の有無を検出し、ある一定以上の台数の再生装置によって同一の
- 15 媒体識別情報の記録媒体の再生が検出された場合には、当該記録媒体を指示する少なくとも媒体識別情報または識別メッセージを媒体リポケーション・リストに追加する更新を行う著作権管理方法である。

- 請求の範囲第41項の発明は、時刻情報に基づいて生成され、所定の機構で読み出された場合に著作権管理者が許可する暦まで所定の機構を
- 20 有する機器において再生動作を制限するシグネチャ・データが電子透かしとして埋め込まれているビデオコンテンツのデータが記録されている記録媒体を再生する再生方法であって、再生された際に、記録媒体からシグネチャ・データを検出するシグネチャ・データ検出ステップと、検出されたシグネチャ・データに基づいて、所定の機構を有する機器内に
- 25 再生の制限を行う暦情報であるシグネチャ・データのリストを生成させるリスト生成ステップと、リストに含まれている限り、所定の機構を有

する機器において、著作権管理者が許可する暦までシグネチャ・データが記録された記録媒体の再生動作を制限する再生制限ステップを有する再生方法である。

請求の範囲第 4 5 項の発明は、ビデオコンテンツのデータが記録されている記録媒体を再生する再生装置であって、再生された際に、ビデオコンテンツのデータに電子透かしとして埋め込まれている、時刻情報に基づいて生成され、著作権管理者が許可する暦まで再生動作を制限するシグネチャ・データを検出するシグネチャ・データ検出部と、検出されたシグネチャ・データに基づいて、再生の制限を行う暦情報であるシグネチャ・データのリストを生成させるリスト生成部と、リストに含まれている限り、著作権管理者が許可する暦までシグネチャ・データが記録された記録媒体の再生動作を制限する制御部とを有する再生装置である。

請求の範囲第 4 9 項の発明は、複数の再生装置と著作権管理者の認可を受けた著作権管理サーバとがネットワークを介して接続された著作権管理システムにおける著作権管理方法において、時刻情報に基づいて生成され、所定の機構で読み出される場合に著作権管理者が許可する暦まで所定の機構を有する機器において再生動作を制限するシグネチャ・データを、ビデオコンテンツに対して電子透かし情報として埋め込み、機器のそれぞれは、ビデオコンテンツを再生する際に、シグネチャ・データを検出し、検出されたシグネチャ・データに基づいて、再生の制限を行う暦情報であるシグネチャ・データのリストを生成し、リストに含まれている限り、機器において、著作権管理者が許可する暦までシグネチャ・データが記録された記録媒体の再生動作を制限する著作権管理方法である。

この発明では、タイトル情報またはタイトルメッセージを記録媒体のビデオコンテンツのデータに電子透かし情報として埋め込む記録方法と、

記録媒体のビデオコンテンツのデータが記録される領域と異なる記録領域に記録する記録する。再生装置が異なる2つの記録方法で記録されたタイトル情報またはタイトルメッセージをそれぞれ読み取り、読み取ったタイトル情報またはタイトルメッセージ同士を比較することで、タイトルが一致しない場合には、不正な記録媒体として、再生を制限することができる。

また、この発明では、記録媒体にその記録媒体を一意に識別する媒体識別情報を記録し、再生装置が媒体識別情報と媒体リポケーション・リストとを比較することで、媒体リポケーション・リストのリポークすべき記録媒体と媒体識別情報で一意に識別された記録媒体とが一致した場合には、不正な記録媒体として、再生を制限することができる。

また、この発明では、記録媒体に電子透かしとしてシグネチャ・データを埋め込むようにし、機器がシグネチャ・データを読み取り、機器内で時刻情報を基に生成されたシグネチャ・データのリストとを比較することで、一致した場合には、著作権管理者が許可しない期間に再生された不正な記録媒体として、再生を制限することができる。

図面の簡単な説明

第1図は、この発明の第1の実施形態によるデジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成（左部分）の一例を示す略線図である。第2図は、この発明の第1の実施形態によるデジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成（真ん中部分）の一例を示す略線図である。第3図は、この発明の第1の実施形態によるデジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成（右部分）の一例を示す略線図である。第4図は、この

発明の第 1 の実施形態によるデジタル・ビデオ・ディスク内のデータ記録領域の構成の一例を示す略線図である。第 5 図は、この発明の第 1 の実施形態によるデジタル・ビデオ・ディスクを再生するデジタル・ビデオ・ディスク再生装置の構成の一例を示す略線図である。第 6 図は、この発明の第 1 の実施形態によるデジタル・ビデオ・ディスクの編集制作工程の流れを示す略線図である。第 7 図は、この発明の第 1 の実施形態によるデジタル・ビデオ・ディスクの製造工程の流れを示す略線図である。第 8 図は、この発明の第 1 の実施形態によるデジタル・ビデオ・ディスクの再生装置における処理の流れ（前半部分）を示す略線図である。

第 9 図は、この発明の第 1 の実施形態によるデジタル・ビデオ・ディスクの再生装置における処理の流れ（後半部分）を示す略線図である。第 10 図は、この発明の第 1 の実施形態での映画の上映期間、正規のデジタル・ビデオ・ディスクの発売時期および違法複製 DVD の再生制限期間との関係の一例を示す略線図である。第 11 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成（左部分）の一例を示す略線図である。第 12 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成（真ん中部分）の一例を示す略線図である。第 13 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成（右部分）の一例を示す略線図である。第 14 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスク内のデータ記録領域の構成の一例を示す略線図である。第 15 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクを再生するデジタル・ビデオ・ディスク再生装置の構成の一例を示す略線図である。第 16 図は、この発明の第 2 の実施

形態によるデジタル・ビデオ・ディスクの編集制作工程の流れを示す略線図である。第 17 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクの製造工程の流れを示す略線図である。第 18 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクの再生装置における処理の流れ（前半部分）を示す略線図である。第 19 図は、この発明の第 2 の実施形態によるデジタル・ビデオ・ディスクの再生装置における処理の流れ（後半部分）を示す略線図である。第 20 図は、この発明の第 2 の実施形態によるフィルム電子透かしチェックの処理の流れを示す略線図である。

10

発明を実施するための最良の形態

まず、この発明の第 1 の実施形態について図面を参照しながら詳細に説明する。第 1 図～第 3 図は、デジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成の一例を示す。作図スペースの制約によって、全体のシステムの構成を第 1 図～第 3 図に分割している。

コンテンツ所有者 10 は、ビデオコンテンツの著作権を所持しており、これをデジタル・ビデオ・ディスク化して販売し利益を得ることを目的としてデジタル・ビデオ・ディスクの量産を発注することを意図している人あるいは団体である。

管理機構 20 は、著作権保護技術の管理機構であり、コンテンツ所有者 10 より依頼を受け、正規の契約関係にあるデジタル・ビデオ・ディスクの編集制作工程、製造工程、および再生装置へ著作権保護技術を運用するための技術・情報を提供し、かつこれを適正に管理し、デジタル・ビデオ・ディスクの不正コピーを排除するための機能を持つ団体である。

編集制作工程 30 は、コンテンツ所有者 10 から依頼されたビデオコンテンツの編集制作工程であり、デジタル・ビデオ・ディスクの編集スタジオなどに設置される。マスタリング工程 40 は、デジタル・ビデオ・ディスクの大量複製のための原盤を作る工程であり、ディスク製造工場内などに設置される。ディスク量産工程 50 は、デジタル・ビデオ・ディスクの大量生産工程であり、ディスク製造工場内などに設置される。

デジタル・ビデオ・ディスク 60 は、大量生産された読み出し専用のデジタル・ビデオ・ディスクメディアであり、ビデオ・オーディオ信号が主に記録される。デジタル・ビデオ・ディスク再生装置 70 は、デジタル・ビデオ・ディスク 60 の再生装置である。

ビデオコンテンツの発行 11 は、デジタル・ビデオ・ディスク 60 へ記録するためのビデオコンテンツを発行する。第 1 図～第 3 図では、管理機構 20 を介しているが、コンテンツ所有者 10 から編集制作工程 30 へ直接ビデオコンテンツを送ることも可能である。不正コピーの流通調査 12 は、不正コピーの流通調査機構である。ここでいう不正コピーの流通調査とは、市場に流通する違法に作成・製造された複製メディアの調査をする行為である。現状は委託された調査会社による市場調査が行われている。量産枚数の発行 13 は、コンテンツ所有者 10 が発注するタイトルのデジタル・ビデオ・ディスク 60 の量産枚数を指定する。第 1 図から第 3 図では、管理機構 20 を介しているが、コンテンツ所有者 10 から編集制作工程 30 に直接量産枚数を指定することも可能である。

GUID の発行 21 は、タイトルごとに配布されるグローバル・ユニーク ID (GUID; Global Unique ID) を発行する。GUID は、ビデオコンテンツのタイトルを示すタイトル情報として利用され、例えば

管理機構 20 の認可を受けた著作権管理サーバからネットワークを介して提供される。ディスク・キーの発行 22 は、コンテンツ鍵を導くための鍵情報の一つであり、デジタル・ビデオ・ディスク 60 へ予め記録されるディスク・キーを発行する。

- 5 フィジカル・インデックスの発行 23 は、ディスクメディアが再生専用メディアであることを識別することを目的として、デジタル・ビデオ・ディスク 60 へ予め記録されるフィジカル・インデックスを発行する。第 1 の実施形態では、コンテンツ鍵を導くための鍵情報の一つとしても利用される。フィジカル・インデックスは再生専用メディアにのみ
- 10 記録され、通常のデータ領域とは異なるチャンネルに複製困難な方法で記録される。フィジカル・インデックスをデジタル・ビデオ・ディスク 60 に記録することにより、正規の工程を経て製造されたディスク・メディアであることが判別可能となる。

- デバイス／ディスク・リボケーション・リストの発行 25 は、違法に
- 15 作成・製造されたビデオコンテンツの再生装置、または、ビデオコンテンツを特定するためのデータを発行する。不正コピー監視 26 は、市場に流通する違法に作成・製造された複製メディアをビデオコンテンツの再生装置から収集したデータに基づいて検出する監視機構である。

- グローバル・シリアル・ナンバの発行 27 は、量産枚数の発行 13 の
- 20 発行者から発行されたディスクの量産枚数に応じて、量産するディスクへ記録されるグローバル・シリアル・ナンバを発行する。グローバル・シリアル・ナンバは、全タイトルを通じたシリアル番号であり、これによりディスク毎に固有の番号が割り振られる。グローバル・シリアル・ナンバは、一連のディスク毎に各ディスクを一意に識別するディスク識
- 25 別番号として利用される。

デバイス ID & デバイス・キーの発行 28 は、デジタル・ビデオ・デ

ディスク再生装置 70 内の不揮発性メモリに記憶されるデバイス ID とデバイス・キーを発行する。デバイス ID はデジタル・ビデオ・ディスク 60 へ予め記録されるデバイス・リポケーション・リストによってデジタル・ビデオ・ディスク再生装置 70 をリポークする際に再生装置を特定するために利用される。また、デバイス ID はデバイス・キーおよびデジタル・ビデオ・ディスク 60 に予め記録されるデバイス・リポケーション・リストから、デジタル・ビデオ・ディスク 60 に予め記録されるディスク・キーの読み出し方法を取得する際に利用される。

ビデオ WM エンベッタ 31 は、ビデオコンテンツへ電子透かし情報を埋め込むための装置である。電子透かしは、静止画や動画などのデジタルコンテンツ中にコンテンツのコピー世代の管理に関する情報や著作権者の情報などの付加情報を埋め込む技術である。電子透かしは、例えばスペクトル拡散に基づく方式により埋め込まれる。この発明で利用される電子透かしは、具体的には、視覚上ほとんど感知できず、且つ埋め込み後にビデオコンテンツが劣化しないものである。なお、図中では、電子透かしを WM と略して示す。

ビデオ WM エンベッタ 31 は、GUID のハッシュ値を計算してハッシュ値を電子透かし情報としてビデオ信号へ埋め込む。ビデオ電子透かしとして埋め込まれた値と、後述する BCA 62 へ記録された値との相関を無くすためにハッシュ値が利用される。ここでいうハッシュ値は、ハッシュ関数などの一方向性関数（同じ出力値になる任意の 2 つの異なる入力を発見することが計算量的に実行不可能な関数）により求められる値である。GUID のハッシュ値は、GUID の真正性の保証に必要となるタイトルメッセージとして利用される。

MPEG 2 エンコーダ 32 は、ビデオ圧縮エンコーダである。ここでは、MPEG (Moving Picture Experts Group) 2 方式を例示するが、

採用される圧縮方式はM P E G 2方式に限らない。ファイルシステムで管理可能なファイルを構成する作業を含み、ボリューム・デスクリプタにはG U I Dが記録される。

ビデオ・エンクリプタ 4 1 は、ディスク・キーおよびフィジカル・インデックスから導出されるコンテンツ鍵によりビデオコンテンツを暗号化する工程である。フォーマッタ 4 2 は、暗号化されたビデオコンテンツ、これを暗号化するために利用したディスク・キーとフィジカル・インデックス、違法に複製されたディスクを特定するためのディスク・リボケーション・リスト、違法に製造または改造された再生装置を特定するためのデバイス・リボケーション・リストから、デジタル・ビデオ・ディスク 6 0 を大量に製造するための原盤を作成する工程である。レプリケータ 5 1 は、原盤からデジタル・ビデオ・ディスク 6 0 を大量に複製する製造工程である。

コンテンツ保護システム 7 1 は、著作権保護技術の制御メカニズムであり、デバイス I D、デバイス・キー、ディスク・リボケーション・リストと再生したデジタル・ビデオ・ディスク 6 0 のグローバル・シリアル・ナンバを記憶する機構、内蔵するセキュア・タイマを較正する機構、および、一定の条件で再生メディアのグローバル・シリアル・ナンバをデジタル・ビデオ・ディスク再生装置 7 0 のデバイス I Dとともに管理機構 2 0 へ報告する仕組みを備える。また、管理機構 2 0 との接続状態にあるとき、内蔵するセキュア・タイマを較正するとともに発見したフィルム電子透かしステータスを報告する仕組みを備える。さらに、デバイス・リボケーション・リスト、ディスク・リボケーション・リスト、シグネチャ・リストを参照して不正な再生状態を検知して再生制限を実行する機構を有する。

映画フィルムの発行 1 0 1 は、映画館で上映する新作の映画を示す。

映画館で上映された映画をデジタル・ビデオ・カメラ等で撮影し、あるいは、テレシネ変換して入手したビデオ信号をデジタル・ビデオ・ディスク 60 として量産する海賊行為を排除するために、保護したいフィルムコンテンツへ電子透かし技術などを用いてシグネチャ・データを埋め込み、このシグネチャ・データを再生装置内で再現する手段を持たせておくことで不正流出コンテンツを再生装置が特定することが可能となる。

WM付き映画フィルム 102 は、映画会社が映画館へ配給する上映用の映画フィルムである。フィルムの形態が一般的であるが、デジタルシネマの場合は劇場上映用圧縮ビデオ・データとなる。著作権保護技術の管理機構によって指定されたシグネチャ・データが電子透かし技術により埋め込まれている。

セキュア・タイマ 103 は、時間情報の改竄が困難な時計である。シグネチャ・データの生成 104 は、映画フィルムへ電子透かし情報として埋め込み、映画フィルムを特定するためのシグネチャ・データをセキュア・タイマ 103 の時刻情報に基づいて生成する装置である。フィルム WMエンベッタ 105 は、映画フィルムへの電子透かし情報の埋め込み装置である。フィルムのマスターそのものに埋め込む方法と、マスターからの転写時に埋め込む方法がある。タイマ校正 106 は、再生装置に内蔵するセキュア・タイマの時刻を校正する仕組みを備える。

第 4 図は、デジタル・ビデオ・ディスク 60 内のデータ記録領域の構成の一例を示す。フィジカル・インデックス記録領域 61 は、フィジカル・インデックスを記録するための領域である。フィジカル・インデックスは、本来のデータ読み出しに影響せずに多重して記録される。

例えば、主データであるビットやマーク等の幅を変調信号により部分的に変化させ、変化させた部分を副データとして主データに多重して記録することができる。また、主データであるビットやマーク等を記録ト

ラックの中心位置からずらして配置することにより、このズレを副データとして主データに多重して記録する方法なども提案されている。これら記録方法による副データ、すなわち多重部分のデータは、本来のデータであるビットやマーク等の主データの幅やズレなどは、再生装置が光
5 ピックアップで読み取ることで、多重部分に記録されたデータを読み取ることができる。さらに、本来のデータの2値化回路等の出力には影響しない。このような多重記録によるデータ記録は、例えば記録媒体の識別情報の記録による不正コピーの排除などに利用されている。

これらの記録方法では、本来のデータをディスク全領域に渡り読み出
10 して、これをコピーしても、多重部分のフィジカル・インデックスがコピーされないことから、まるごとコピー（ビットバイビットコピー）に効果的とされる。

バースト・カッティング・エリア（Burst Cutting Area；以後、適宜
BCAと称する）であるBCA62には、タイトルを特定するためのG
15 UIDとディスクごとに異なる値となるグローバル・シリアル・ナンバーが記録される。BCAは、データ記録された後でディスクメディアに記録される。BCAは、ディスク状光記録媒体の場合、例えばディスクの内側に形成されているアルミニウム等よりなる反射膜に、記録情報に従って変調したパルスレーザ光を照射することで、半径方向に細長く除去
20 したストライプ（バーコード）を形成し、記録情報に応じて、ディスク最内周の円周に沿って形成することができる。再生装置は、このように形成されたBCAを光ピックアップで読み取ることで、BCAに記録されているデータを取得することができる。コンピュータなどでデータ領域を他の記録媒体にコピーしても、BCAに記録されているデータはコ
25 ピーされないため、例えば、記録媒体のIDデータやデータ領域に記録する暗号化されたコンテンツの鍵データをBCAに記録しておくことで、

不正コピーされた記録媒体によるコンテンツの再生の防止に利用されている。

デバイス・リボケーション・リスト、ディスク・リボケーション・リスト、ディスク・キーは、ビデオコンテンツの記録される領域とは区別された領域、例えばリードインエリア 6 3 に書き換え不可能な状態で記録される。

データエリア 6 4 は、GUID のハッシュ値が電子透かし情報として埋め込まれた暗号化されたビデオコンテンツを記録するデータ領域である。

10 第 5 図は、デジタル・ビデオ・ディスク 6 0 を再生するデジタル・ビデオ・ディスク再生装置 7 0 内の構成の一例を示す。ROM 識別器 7 2 は、デジタル・ビデオ・ディスク再生装置 7 0 へ装着されたディスクが読み出し専用のデジタル・ビデオ・ディスク 6 0 であるか否かを判定するための識別を行う。もし、読み出し専用のデジタル・ビデオ・ディスク 6 0 であると判定されたならばスイッチ S W 1 をオン状態に設定する。
15 そうでなければ、オフ状態に設定する。

デクリプタ 7 3 は、暗号化されたビデオコンテンツの復号を行う。暗号化検出器 7 4 は、デジタル・ビデオ・ディスク再生装置 7 0 がリボークされていないかどうかの確認とデジタル・ビデオ・ディスク 6 0 へ記録されたビデオコンテンツが暗号化記録されているかどうかの検査を行う。
20 検査結果が再生装置がリボークされておらずビデオコンテンツが暗号化記録されていたことを示したならば、スイッチ S W 2 をオン状態に設定する。そうでなければ、オフ状態に設定する。

M P E G 2 デコーダ 7 5 は、ビデオ圧縮を解き、ベースバンド・ビデオ信号へ変換する。ビデオ W M 検出器 7 6 は、ビデオコンテンツに埋め込まれたビデオ電子透かし情報を検出する。電子透かし情報の検出後、
25

BCA 6 2 に記録される GUID のハッシュ値を計算し、このハッシュ値と電子透かし情報を比較する。両者が一致しないことを確認したのならば、スイッチ SW 3 をオフ状態に設定する。両者が一致した場合、または電子透かし情報が未検出の間は、スイッチ SW 3 はオン状態に設定される。

ディスク・リボケーション・チェッカー 7 7 は、BCA 6 2 に記録されたグローバル・シリアル・ナンバのハッシュ値と、再生装置内の不揮発性メモリに記憶されたディスク・リボケーション・リスト内に登録された値とを比較し、同じ値が登録されているか否かを確認する工程である。もし、値が一致したならば、デジタル・ビデオ・ディスク 6 0 は、リボケーションの対象と判定してスイッチ SW 4 をオフ状態に設定する。値の一致が確認されない間は、オン状態に設定される。なお、比較する値は、グローバル・シリアル・ナンバのハッシュ値だけでなく、GUID などの他の情報を組み合わせることもできる。これにより、一意にディスクを特定する確率を高くすることができ、正規ディスクを誤ってリボークしてしまう危険が少なくなる。

ハッシュ関数 7 8 は、グローバル・シリアル・ナンバのハッシュ値を計算するハッシュ関数であり、ディスクにリボークするグローバル・シリアル・ナンバのハッシュ値を登録する場合に使用されるものと同じ関数となる。グローバル・シリアル・ナンバのハッシュ値は、グローバル・シリアル・ナンバの真正性の保証に必要な識別メッセージとして利用される。デジタル・ビデオ・ディスク再生装置 7 0 から管理機構 2 0 へデータが転送される際に、ユーザが視聴したタイトルを特定できなくすることでプライバシーを守れるよう、グローバル・シリアル・ナンバのハッシュ値が利用される。

不揮発性メモリ 7 9 は、再生装置が再生したメディアの記録として、

- グローバル・シリアル・ナンバのハッシュ値を記憶するための不揮発性メモリである。管理機構 20 とデジタル・ビデオ・ディスク再生装置 70 とのネットワーク接続が成立しているときに、この不揮発性メモリ 79 内の再生メディア記録データをデバイス ID 89、デバイス・シリアル・ナンバ 91 とともに管理機構 20 へ転送し、転送後にこの不揮発性メモリ 79 内のデータを消去して空き領域を確保する。ネットワーク接続においては、SSL (Secure Socket Layer) 認証、IPsec (IP security protocol) 暗号化に基づくVPN (Virtual Private Network) などの暗号化通信が行われることなどが想定される。
- 10 バージョン・チェッカー 80 は、デジタル・ビデオ・ディスク 60 に記録されるディスク・リボケーション・リストを不揮発性メモリ 81 へ格納する際に、既に格納されているディスク・リボケーション・リストのバージョンとデジタル・ビデオ・ディスク 60 に記録されているディスク・リボケーション・リストのバージョンとどちらが新しいバージョンであるかの比較を行う。もし、デジタル・ビデオ・ディスク 60 に記録されたデータのバージョンの方が新しいのであれば、スイッチ SW 6
- 15 をオン状態に設定して不揮発性メモリ 81 内のディスク・リボケーション・リストのデータを更新する。
- 不揮発性メモリ 81 は、ディスク・リボケーション・リストを格納するための不揮発性メモリである。ディスク・リボケーション・リストは、管理機構 20 とデジタル・ビデオ・ディスク再生装置 70 とのネットワーク接続が確立している状態において、管理機構 20 から転送される場合もあり、この時もメディアから更新されるのと同じプロセスで不揮発性メモリ 81 内のデータの更新が行われる。
- 20
- 25 セキュア・タイマ 82 は、デジタル・ビデオ・ディスク再生装置 70 に内蔵される改竄が困難なタイマである。出力する時刻情報をもとにシ

グネチャ・リストが生成される。タイマの時刻情報は管理機構 20 とデジタル・ビデオ・ディスク再生装置 70 とのネットワーク接続が確立している状態において、管理機構 20 内のセキュア・タイマ 103 との同期がとられ較正される場合もある。

- 5 シグネチャ・リスト生成器 83 は、セキュア・タイマ 82 の出力する時刻情報より遡って複数分の、例えば 100 タイトル分の映画フィルムのシグネチャ・データを生成してシグネチャ・リストを作成する。この 100 タイトルは例えば上映中の新作の映画であり、まだデジタル・ビデオ・ディスク 60 として量産・販売されていないタイトルである。もし、再生装置がこれを再生したとしたら、それは不正に流出したコンテンツであるとみなされる。

フィルムWM検出器 84 は、再生中のビデオコンテンツに電子透かし情報として埋め込まれたフィルム電子透かしステータスを検出する工程である。

- 15 比較器 88 は、フィルムWM検出器 84 で検出されたフィルム電子透かしステータスとシグネチャ・リスト生成器 83 内に格納された不正に流出したコンテンツであることを特定するためのシグネチャ・リストとを比較する工程である。フィルムWM検出器 84 の検出が完了していない間は、スイッチ SW5 はオン状態に設定される。フィルムWM検出器 20 84 の検出が完了し、かつそのステータスがシグネチャ・リスト生成器 83 に格納されたシグネチャ・リストに登録済みであれば、再生コンテンツは不正に流出したコンテンツであるとみなし、スイッチ SW5 をオフ状態に設定することでコンテンツの再生動作を中断する。あるいは、不正なコンテンツを再生していることを示すメッセージを再生画面へスーパーインポーズして、利用者へ告知する。

デバイス ID 89 は、デジタル・ビデオ・ディスク再生装置 70 の識

別データである。再生装置の製造業者単位、あるいは機種単位で、固有の識別番号が配布される。

デバイス・キー 90 は、デバイス ID 89 とディスク・リボケーション・リストから計算されるデータと組み合わせることでデジタル・ビデオ・ディスク 60 へ記録された暗号化等により秘匿されたディスク・キーを導出する。

デバイス・シリアル・ナンバ 91 は、デジタル・ビデオ・ディスク再生装置 70 の製造業者によって配布される一連のデバイス毎にデバイスを特定するための製造シリアル番号である。

10 スイッチ SW1 は、ROM 識別器 72 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW2 は、暗号化検出器 74 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW3 は、ビデオ WM 検出器 76 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。

15 スイッチ SW4 は、ディスク・リボケーション・チェッカー 77 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW5 は、比較器 88 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW6 は、バージョン・チェッカー 80 の判定結果に基づいてディスク・リボケーション・リストの格納を制御するためのスイッチである。

20

< 1. 編集制作工程の説明 >

第 6 図は、デジタル・ビデオ・ディスク 60 の編集制作工程の流れを示す。第 6 図に示すデジタル・ビデオ・ディスク 60 の編集制作工程の処理フローをもとに、第 1 図～第 3 図の全体システム構成を示すブロック図を参照しながら説明する。

25

コンテンツ所有者 10 よりデジタル・ビデオ・ディスク化を希望する

ビデオコンテンツを受け取ることで編集制作プロジェクトが発生する。デジタル・ビデオ・ディスク制作のための編集制作プロジェクトが起これると、編集制作工程 30 は管理機構 20 に対して GUID の発行を要請する（ステップ S 11）。なお、図中の CA は管理機構 20 を示す。

- 5 この要請を受けた管理機構 20 はタイトルごとに固有の GUID を発行する（ステップ S 12）。GUID の発行を受けた編集制作工程 30 はステップ S 14 においてビデオコンテンツへ GUID のハッシュ値を埋め込む（ステップ S 13）。

- 10 管理機構 20 とのライセンス契約に基づいて提供を受けたビデオ WM エンベッタ 31 では、GUID のハッシュ値を計算した上で、そのハッシュ値を電子透かし情報としてビデオコンテンツのビデオ信号へ埋め込む（ステップ S 14）。

- 15 ステップ S 10、すなわち、ステップ S 11 からステップ S 14 において、編集制作工程 30 と管理機構 20 とは SSL、IPsec 技術などを利用した VPN を構成するものとし、セキュアなネットワーク接続によるデータの送受信が可能な状態にあるものとする。

- 20 ハッシュ値を電子透かし情報として埋め込んであるビデオ信号とともに、ビデオコンテンツ内のオーディオ信号、字幕などのサブタイトル、ビデオコンテンツのアクセスを容易とするためのメニュー、およびインタラクティブ機能を実現するためのデータやプログラムをエンコードする（ステップ S 15）。

- 25 各ファイル・データを多重化し、ファイルシステム管理情報であるボリューム・デスクリプタの中に GUID を記録する（ステップ S 16）。ディスク製造工程へ作業を引き継ぐために、HD-DVD ディスク・イメージをマスタフォーマットへ書き込む（ステップ S 17）。

< 2. ディスク製造工程の説明 >

第7図は、デジタル・ビデオ・ディスク60の製造工程の流れを示す。第7図に示すデジタル・ビデオ・ディスク60の製造工程の処理フローをもとに、第1図～第3図の全体システム構成を示すブロック図と、第4図のディスクメディア関係図を参照しながら説明する。

- 5 HD-DVDディスク・イメージを編集制作工程30から受け取る
 (ステップS21)。ボリューム・デスクリプタを展開してGUID
 を読み出す。ここで得られたGUIDをディスク製造工場から管理機
 構20へ転送する(ステップS22)。

- コンテンツ所有者10は編集制作工程30に対する編集制作用ビデオ
10 コンテンツを渡すとともにディスク製造工場に対してディスク量産の発
 注を実施しており、その際に発注枚数も指定される(ステップS23)。

- コンテンツ所有者10からディスク量産の発注を受けたディスク製造
 工場は、GUIDと発注枚数を管理機構20へ転送し、製造するディ
 スク1枚1枚に書き込むグローバル・シリアル・ナンバの発行を要求す
15 る(ステップS24)。

- 管理機構20ではディスク製造工場から受け取ったGUIDから、
 ビデオコンテンツのタイトルを特定する。また、受け取った発注枚数か
 ら製造するディスクメディアが全タイトルにわたって1枚1枚が固有の
 シリアル番号が記録できるように未使用のグローバル・シリアル・ナン
20 バを受注枚数分だけ厳正に算出する(ステップS25)。

- 管理機構20はディスク製造工場に対して、ディスク製造の許諾すな
 わちHD-DVDディスク・イメージを暗号化するために必要なディス
 ク・キー、グローバル・シリアル・ナンバー式、デバイス・リボケーシ
 ョン・リスト、ディスク・リボケーション・リストを転送する(ステッ
25 プS26)。デバイス・リボケーション・リストは不正に製造されたデ
 ィスク再生装置において正規ディスクメディアの再生が制限されるよう

にするためのデータである。ディスク・リボケーション・リストは不正に製造されたディスクメディアを正規のディスク再生装置において再生が制限されるようにするためのデータである。

ディスク製造工場は、編集制作工程 30 から受け取った HD-DVD
5 ディスク・イメージに、管理機構 20 から受け取ったこれらのデータを組み合わせ、さらに管理機構 20 とのライセンス契約に基づいて提供された暗号化技術を利用して HD-DVD ディスク・イメージを暗号化してディスク・マスター（原盤）を作成する（ステップ S 27）。

ステップ S 20、すなわち、ステップ S 24 からステップ S 27 にお
10 いて、ディスク製造工場と管理機構 20 とは SSL、IPsec 技術などを利用した VPN を構成するものとし、セキュアなネットワーク接続によるデータの送受信が可能な状態にあるものとする。

ディスク・マスター（原盤）からディスクメディアを大量生産する
（ステップ S 28）。製造されたディスクメディアへ BCA を焼きこむ。
15 BCA には、タイトルを特定できる GUID と 1 枚 1 枚が異なる値を持つグローバル・シリアル・ナンバが記録される（ステップ S 29）。

<3. ディスク再生装置の説明>

第 8 図および第 9 図は、デジタル・ビデオ・ディスク 60 の再生装置における処理の流れを示す。作図スペースの制約によって、処理の流れ
20 を第 8 図および第 9 図に分割している。第 8 図および第 9 図に示すデジタル・ビデオ・ディスク 60 の再生装置の処理フローをもとに、第 5 図の、デジタル・ビデオ・ディスク再生装置 70 の構成を示すブロック図を参照しながら、ディスクメディアが再生装置へ装着された後の再生装置の動作を説明する。

25 まず、再生装置は、装着されたディスクメディアからフィジカル・インデックス記録領域 61 を読み出す（ステップ S 30）。フィジカル・

インデックス記録領域 6 1 の読み出し方法は再生装置および再生装置に利用される部品の製造業者が管理機構 2 0 と正規の契約を結ぶことにより提供される。

- 読み出しにより、フィジカル・インデックスが正しく検出されるかどうかを判定する（ステップ S 3 1）。再生装置が正しくフィジカル・インデックスを検出できなかった場合、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。ここで、再生装置は再生専用ディスクメディアのみを再生するものとしたが、フィジカル・インデックスの存在しない記録型ディスクメディアを再生可能な場合は、
10 その記録型ディスクメディアを再生するための処理へ移行することも想定される。

- 再生装置が正しくフィジカル・インデックスを検出した場合、BCA データを読み、GUID とグローバル・シリアル・ナンバを取得する（ステップ S 3 2）。グローバル・シリアル・ナンバのハッシュ値を計算し、不揮発性メモリ 7 9 に記憶されている再生ディスク・メディア・リストを検索する（ステップ S 3 3）。
15

- 再生ディスク・メディア・リスト内にハッシュ値が存在すればステップ S 3 5 へ進む。再生ディスク・メディア・リスト内にハッシュ値が存在しなければ、そのハッシュ値を不揮発性メモリ 7 9 へ格納する（ステップ S 3 4）。このリストは、デジタル・ビデオ・ディスク再生装置 7
20 0 と管理機構 2 0 とがセキュアにネットワーク接続されているときにデジタル・ビデオ・ディスク再生装置 7 0 から管理機構 2 0 へ転送され、メモリの空き状況に応じて、転送後に不揮発性メモリ 7 9 に記録されたリストは消去される。

- 25 グローバル・シリアル・ナンバのハッシュ値で、不揮発性メモリ 8 1 に記憶されているディスク・リボケーション・リストを検索する（ステ

ップS 3 5)。ディスク・リボケーション・リスト内にハッシュ値が存在すれば、再生ディスクメディアはリボケーションの対象と判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。

- 5 ディスク・リボケーション・リスト内にハッシュ値が存在しなければ、リードイン領域のデバイス・リボケーション・リストとディスク・リボケーション・リストと暗号化等により秘匿されたディスク・キーとを読み出す（ステップS 3 6）。これらの情報はディスクに記録された暗号化ビデオコンテンツを復号するために必要とされる。この暗号化ビデオ
- 10 コンテンツの復号技術は再生装置および再生装置に利用される部品の製造業者が管理機構20と正規の契約を結ぶことにより提供される。

- デバイス・リボケーション・リストとディスク・リボケーション・リストが正しく読み出せたか、再生装置がデバイス・リボケーション・リストによるリボーク対象ではなく暗号化等により秘匿されたディスク・
- 15 キーが正しく読み出せたかどうかを判定する（ステップS 3 7）。デバイス・リボケーション・リスト、ディスク・リボケーション・リストが正しく読み出せなかった、あるいは再生装置がデバイス・リボケーション・リストのリボーク対象とされ暗号化等により秘匿されたディスク・キーを正しく読み出すことが出来なかった場合など、ビデオコンテンツ
- 20 が適正に暗号化記録されていないと判断される場合には、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。

- デバイス・リボケーション・リスト、ディスク・リボケーション・リストを正しく読み出すことが出来、さらに暗号化等により秘匿されたディスク・キーを正しく読み出すことが出来、再生装置がデバイス・リボ
- 25 ケーションの対象とされていないことが確認された場合には、ディスク・リボケーション・リストの更新を行う（ステップS 3 8）。このリ

ストにはバージョン情報が含まれている。不揮発性メモリ 8 1 内に記憶されている過去のディスク・リボケーション・リストのバージョンよりも新しいディスク・リボケーション・リストを取得した場合には、不揮発性メモリ 8 1 内のリストを更新する。メモリ内には複数のバージョンのディスク・リボケーション・リストを記憶させ、古いバージョンのデータから順番に消去するという F I F O (First-In First-Out) 構造をとることもありうる。データ領域を読み出し、復号された暗号化ビデオコンテンツの再生を開始する (ステップ S 3 9)。

再生開始後、ある時間が経過するまでビデオ信号に埋め込まれているビデオ電子透かしが検出されるのを待つ (ステップ S 4 0)。ある一定時間が経過しても、または、ある一定量のストリームを処理してもビデオ電子透かしが検出されなかった場合、再生ディスクメディアは不正な編集制作工程によってつくられたビデオコンテンツであると判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。このビデオ電子透かしの検出技術は再生装置および再生装置に利用される部品の製造業者が管理機構 2 0 と正規の契約を結ぶことにより提供される。

ある一定時間内に、もしくは、ある一定処理量内でビデオ電子透かしが検出されたならば、その電子透かし情報が G U I D のハッシュ値と同じ値を示すか否かを確認する (ステップ S 4 1)。一致しなかった場合、再生ディスクメディアは不正な編集制作工程によってつくられたビデオコンテンツである、あるいは不正な製造工程で製造されたディスク・メディアであると判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。一致した場合には、再生動作を継続する (ステップ S 4 2)。

ビデオコンテンツの再生中に、シグネチャ・リスト生成器 8 3 内にシ

グネチャ・リストを生成する（ステップS 4 3）。シグネチャ・リストは、コンテンツ所有者10が劇場で新作の映画を公開する際に、その新作映画がディスクメディアとして販売される以前に海賊行為により製造されたディスクメディアが販売されることで、新作映画の興行収入を獲得する機会と正規ディスクメディアの販売収入を獲得する機会を損なうことを防ぐことを目的として設けられたものであり、興行中もしくは興行予定の映画を特定するためシグネチャ・データが複数記録されたデータベースである。このシグネチャ・リストの生成方法は再生装置および再生装置に利用される部品の製造業者が管理機構20と正規の契約を結ぶことにより提供される。

フィルムWM検出器84によるフィルム電子透かしの検出が実行される。フィルム電子透かしが検出されたならば、そのステータスでシグネチャ・リスト生成器83内に格納されているシグネチャ・リストを検索し一致したシグネチャ・データが登録されているか確認する（ステップS 4 4）。もし登録されていることが確認されたならば、再生ディスクメディアは劇場で上映された作品を不正に取得し、これをソースとして編集制作・製造されたビデオコンテンツであると判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。登録が無ければ正規の契約に基づいて編集制作・製造されたディスク・メディアであることが確認され、通常の再生動作が保証される。このフィルム電子透かしの検出技術は再生装置および再生装置に利用される部品の製造業者が管理機構20と正規の契約を結ぶことにより提供される。

以上説明したこの発明の第1の実施形態では、デジタル・ビデオ・ディスク60にGUIDとGUIDのハッシュ値とが、異なる2種類の記録方法で記録される。GUIDは、ディスクメディアのBCAに記録される。GUIDのハッシュ値は、デジタル・ビデオ・ディスク化を行う

- ビデオコンテンツに電子透かし情報として埋め込まれる。デジタル・ビデオ・ディスク再生装置 70 は、BCA から GUID を読み取り、読み取った GUID のハッシュ値と、ビデオコンテンツに埋め込まれた電子透かし情報とを比較して、一致したら再生動作を行う。これにより、管理機構 20 の認可を受けた編集制作工程 30 でビデオ編集されたコンテンツが、同じく管理機構 20 の認可を受けたディスク製造工程（マスタリング工程 40、ディスク量産工程 50）で製造されたデジタル・ビデオ・ディスク 60 へ記録されたことを、デジタル・ビデオ・ディスク再生装置 70 が確認できる。
- 10 したがって、不正に入手したビデオ信号を、不正な編集制作工程でビデオ編集し、ディスク製造工場で製造し配布されたディスクメディアをデジタル・ビデオ・ディスク再生装置 70 が識別可能であり、これに対して再生制限を加えることが可能となる。

- 通常、CCI（Copy Control Information）を電子透かし情報として
- 15 ビデオ信号へ埋め込むのが一般的であるが、これは電子透かし情報が攻撃により検出不可能とされることで無効化される。この発明の第 1 の実施形態では、電子透かし情報として埋め込まれた GUID の情報が正しく検出され、ディスクメディアの BCA へ別途記録済みの GUID の情報と比較し、一致が確認されたことを持って再生許可されるのであるから、電子透かし情報を検出不可能とするための攻撃は全く意味をなさな
- 20 い。したがって、電子透かし技術に対する攻撃への対処が不要であり、適用する電子透かし技術が簡易なものとなる。このことは、新技術を適用する再生装置の低コスト化に貢献する。

- また、この発明の第 1 の実施形態では、マスタリング工程 40 において、管理機構 20 から発行されたフィジカル・インデックスがデジタル・ビデオ・ディスク 60 に記録される。このフィジカル・インデック
- 25

スは、再生専用ディスクメディアに本来のデータ読み出しに影響せずに多重記録されている。デジタル・ビデオ・ディスク再生装置 70 は、再生したディスクからフィジカル・インデックスが検出された場合に再生動作を行うように構成されている。これにより、管理機構 20 の認可を受けたディスク製造工場で製造された再生専用ディスク・メディアであるか否かを、デジタル・ビデオ・ディスク再生装置 70 が確認することを可能とする。

また、デジタル・ビデオ・ディスク 60 に記録されたビデオコンテンツは暗号化されている。これにより、デジタル・ビデオ・ディスク再生装置 70 は、不正に入手したビデオ信号を、不正なディスク製造工場で製造し配布されたディスク・メディアであるか否かを、ROM 識別器 72 でのフィジカル・インデックスの検出による再生専用ディスク・メディアであるかの確認と、暗号化検出器 74 によるデジタル・ビデオ・ディスク 60 のビデオコンテンツが暗号化記録されたものであるかの確認との 2 つの手段で識別可能であり、これに対して再生制限を加えることが可能となる。

また、この発明の第 1 の実施形態では、指定された枚数以上のディスクを余分に製造しようとする、グローバル・シリアル・ナンバが必ず重複することになる。この重複は、デジタル・ビデオ・ディスク再生装置 70 とネットワーク接続される管理機構 20 の管理サーバ等により監視することで、検出が可能である。したがって、管理機構 20 の認可を受けたディスク製造工場において、正規に発注された枚数を越えたディスク製造が行われないように管理することが可能となる。さらにグローバル・シリアル・ナンバのハッシュ値をネットワークへ流しても、ハッシュ値からタイトルを特定することができず、利用者のプライバシーを保護することが可能となる。

また、この発明の第1の実施形態では、映画館等で上映されるフィルムコンテンツには、フィルムWMエンベッタ105においてシグネチャ・データが電子透かしにより埋め込まれている。デジタル・ビデオ・ディスク再生装置70は、ディスクの再生の際、シグネチャ・リスト生成器83において時間情報をもとにシグネチャ・リストを生成し、フィルムWM検出器84においてフィルムコンテンツに埋め込まれた電子透かし情報を読み取る。そして比較器88において、シグネチャ・リストとシグネチャ・データとを比較し、両者が一致した場合には、再生を停止する。これにより、再生したディスクメディアが新作上映中の映画館から不正に流出されたビデオ信号から製造された海賊版ディスク・メディアであるか否かをデジタル・ビデオ・ディスク再生装置70は確認することが可能となり、これに対して再生制限を加えることが可能となる。

以下に、この発明の第1の実施形態によるシグネチャ・リスト、シグネチャ・データを利用した再生制限について図面を参照しながら説明する。第10図は、フィルムコンテンツとしての映画の上映期間、正規のデジタル・ビデオ・ディスクの発売時期および違法複製DVDの再生制限期間との関係の一例を示す。第10図に示すように、例えば、タイトルA, B, C, ...の順に新作の映画が劇場で公開され、その後、正規DVD発売予定日に示すように、タイトルA, B, C, ...の順に正規のデジタル・ビデオ・ディスクが発売されるものとする。

第10図に示す「再生日」は、この発明の第1の実施形態によるデジタル・ビデオ・ディスク再生装置70により、DVDを再生した日を表す。例えば、正規のデジタル・ビデオ・ディスクが発売されるまで違法複製DVDの再生を制限するものとし、第10図に示すように、デジタル・ビデオ・ディスク再生装置70内のシグネチャ・データの生成範囲が例えば再生日から200日であるものとする。

この場合、最初の再生時には、その再生日から200日以内に正規DVDの発売予定日が含まれるタイトルA、Bが再生制限タイトルとされ、デジタル・ビデオ・ディスク再生装置70内でタイトルA、Bを特定するシグネチャ・データが生成される。同様に、2回目の再生日には、タイトルA、B、Cが再生制限タイトルとされ、デジタル・ビデオ・ディスク再生装置70内でタイトルA、B、Cを特定するシグネチャ・データが生成される。

3回目の再生日には、タイトルAの正規のDVDが発売済みであるため、タイトルB、Cが再生制限タイトルとされ、デジタル・ビデオ・ディスク再生装置70内でタイトルB、Cを特定するシグネチャ・データが生成される。同様に、4番目の再生日には、タイトルCが再生制限タイトルとされ、デジタル・ビデオ・ディスク再生装置70内でタイトルCを特定するシグネチャ・データが生成される。5番目以降も、同様に再生制限タイトルが決定され、再生を制限するタイトルを特定するシグネチャ・データがデジタル・ビデオ・ディスク再生装置70内で生成される。

このように生成された複数のシグネチャ・データによるシグネチャ・リストと、再生したDVDの電子透かしにより埋め込まれたシグネチャ・データとを比較し、一致した場合にデジタル・ビデオ・ディスク再生装置70によりディスクの再生が制限される。

上述した第1の実施形態は、ディスク固有の番号を、通し番号で割り当てたグローバル・シリアル・ナンバとして仮定したが、ディスク固有の番号をランダムに割り当てることも可能である。この発明の第2の実施形態は、上述した第1の実施形態において、ディスク固有の番号をランダムに割り当てたものである。

以下、第2の実施形態について図面を参照しながら詳細に説明する。

第 1 1 図～第 1 3 図は、デジタル・ビデオ・ディスクの制作工程、製造工程、および再生装置からなる全体のシステム構成の一例を示す。作図スペースの制約によって、全体システムを第 1 1 図～第 1 3 図に分割している。

- 5 コンテンツ所有者 1 0 は、ビデオコンテンツの著作権を所持しており、これをデジタル・ビデオ・ディスク化して販売し利益を得ることを目的としてデジタル・ビデオ・ディスクの量産を発注することを意図している人あるいは団体である。

- 10 管理機構 2 0 は、著作権保護技術の管理機構であり、コンテンツ所有者 1 0 より依頼を受け、正規の契約関係にあるデジタル・ビデオ・ディスクの編集制作工程、製造工程、および再生装置へ著作権保護技術を運用するための技術・情報を提供し、かつこれを適正に管理し、デジタル・ビデオ・ディスクの不正コピーを排除するための機能を持つ団体である。

- 15 編集制作工程 3 0 は、コンテンツ所有者 1 0 から依頼されたビデオコンテンツの編集制作工程であり、デジタル・ビデオ・ディスクの編集スタジオなどに設置される。マスタリング工程 4 0 は、デジタル・ビデオ・ディスクの大量複製のための原盤を作る工程であり、ディスク製造工場内などに設置される。ディスク量産工程 5 0 は、デジタル・ビデオ・ディスクの大量生産工程であり、ディスク製造工場内などに設置される。

- 25 デジタル・ビデオ・ディスク 6 0 は、大量生産された読み出し専用のデジタル・ビデオ・ディスクメディアであり、ビデオ・オーディオ信号が主に記録される。デジタル・ビデオ・ディスク再生装置 7 0 は、デジタル・ビデオ・ディスク 6 0 の再生装置である。

ビデオコンテンツの発行 1 1 は、デジタル・ビデオ・ディスク 6 0 へ

記録するためのビデオコンテンツを発行する。第11図～第13図では、コンテンツ所有者10から編集制作工程30へ直接ビデオコンテンツを送っているが、管理機構20を介して送ることも可能である。不正コピーの流通調査12は、不正コピーの流通調査機構である。ここでいう不正コピーの流通調査とは、市場に流通する違法に作成・製造された複製メディアの調査をする行為である。現状は委託された調査会社による市場調査が行われている。量産枚数の発行13は、コンテンツ所有者10が発注するタイトルのデジタル・ビデオ・ディスク60の量産枚数を指定する。第11図～第13図では、コンテンツ所有者10から編集制作工程30に直接量産枚数を指定しているが、管理機構20を介して指定することも可能である。

GUIDの発行21は、タイトルごとに配布されるグローバル・ユニークID (GUID; Global Unique ID) を発行する。GUIDは、ビデオコンテンツのタイトルを示すタイトル情報として利用され、例えば管理機構20の認可を受けた著作権管理サーバからネットワークを介して提供される。ディスク・キーの発行22は、コンテンツ鍵を導くための鍵情報の一つであり、デジタル・ビデオ・ディスク60へ予め記録されるディスク・キーを発行する。

フィジカル・インデックスの発行23は、ディスクメディアが再生専用メディアであることを識別することを目的として、デジタル・ビデオ・ディスク60へ予め記録されるフィジカル・インデックスを発行する。第2の実施形態では、コンテンツ鍵を導くための鍵情報の一つとしても利用される。フィジカル・インデックスは再生専用メディアにのみ記録され、通常データ領域とは異なるチャネルに複製困難な方法で記録される。フィジカル・インデックスをデジタル・ビデオ・ディスク60に記録することにより、正規の工程を経て製造されたディスク・メデ

ィアであることが判別可能となる。

デバイス／ディスク・リボケーション・リストの発行 25 は、違法に作成・製造されたビデオコンテンツの再生装置、または、ビデオコンテンツを特定するためのデータを発行する。不正コピーの監視 26 は、市場に流通する違法に作成・製造された複製メディアをビデオコンテンツの再生装置から収集したデータに基づいて検出する監視機構である。

デバイス ID & デバイス・キーの発行 28 は、デジタル・ビデオ・ディスク再生装置 70 内の不揮発性メモリに記憶されるデバイス ID とデバイス・キーを発行する。デバイス ID はデジタル・ビデオ・ディスク 60 へ予め記録されるデバイス・リボケーション・リストによってデジタル・ビデオ・ディスク再生装置 70 をリボークする際に再生装置を特定するために利用される。また、デバイス ID はデバイス・キーおよびデジタル・ビデオ・ディスク 60 に予め記録されるデバイス・リボケーション・リストから、デジタル・ビデオ・ディスク 60 に予め記録されるディスク・キーの読み出し方法を取得する際に利用される。

ビデオ WM エンベッタ 31 は、ビデオコンテンツへ電子透かし情報を埋め込むための装置である。ビデオ WM エンベッタ 31 は、GUID のハッシュ値を計算してハッシュ値を電子透かし情報としてビデオ信号へ埋め込む。ビデオ電子透かしとして埋め込まれた値と、後述する BCA 62 へ記録された値との相関を無くすためにハッシュ値が利用される。GUID のハッシュ値は、GUID の真正性の保証に必要となるタイトルメッセージとして利用される。電子透かし、ハッシュ値については、上述した第 1 の実施形態で説明したのでここでは説明を省略する。

MPEG 2 エンコーダ 32 は、ビデオ圧縮エンコーダである。ここでは、MPEG 2 方式を例示するが、採用される圧縮方式は MPEG 2 方式に限らない。ファイルシステムで管理可能なファイルを構成する作業

を含み、ボリューム・デスクリプタにはG U I Dが記録される。

ビデオ・エンクリプタ 4 1 は、ディスク・キーおよびフィジカル・インデックスから導出されるコンテンツ鍵によりビデオコンテンツを暗号化する工程である。フォーマッタ 4 2 は、暗号化されたビデオコンテンツ、これを暗号化するために利用したディスク・キーとフィジカル・インデックス、違法に複製されたディスクを特定するためのディスク・リボケーション・リスト、違法に製造または改造された再生装置を特定するためのデバイス・リボケーション・リストから、デジタル・ビデオ・ディスク 6 0 を大量に製造するための原盤を作成する工程である。レプリケータ 5 1 は、原盤からデジタル・ビデオ・ディスク 6 0 を大量に複製する製造工程である。

コンテンツ保護システム 7 1 は、著作権保護技術の制御メカニズムであり、デバイス I D、デバイス・キー、ディスク・リボケーション・リストと再生したデジタル・ビデオ・ディスク 6 0 のディスク・ユニーク・ナンバを記憶する機構、内蔵するセキュア・タイマを較正する機構、および、一定の条件で再生メディアのディスク・ユニーク・ナンバをデジタル・ビデオ・ディスク再生装置 7 0 のデバイス I D とともに管理機構 2 0 へ報告する仕組みを備える。また、管理機構 2 0 との接続状態にあるとき、内蔵するセキュア・タイマを較正するとともに発見したフィルム電子透かしステータスを報告する仕組みを備える。さらに、デバイス・リボケーション・リスト、ディスク・リボケーション・リスト、シグネチャ・リストを参照して不正な再生状態を検知して再生制限を実行する機構を有する。

映画フィルムの発行 1 0 1 は、映画館で上映する新作の映画を示す。映画館で上映された映画をデジタル・ビデオ・カメラ等で撮影し、あるいは、テレシネ変換して入手したビデオ信号をデジタル・ビデオ・ディ

スク 6 0 として量産する海賊行為を排除するために、保護したいフィルムコンテンツへ電子透かし技術などを用いてシグネチャ・データを埋め込み、このシグネチャ・データを再生装置内で再現する手段を持たせておくことで不正流出コンテンツを再生装置が特定することが可能となる。

- 5 WM付き映画フィルム 1 0 2 は、映画会社が映画館へ配給する上映用の映画フィルムである。フィルムの形態が一般的であるが、デジタルシネマの場合は劇場上映用圧縮ビデオ・データとなる。著作権保護技術の管理機構によって指定されたシグネチャ・データが電子透かし技術により埋め込まれている。
- 10 セキュア・タイマ 1 0 3 は、時間情報の改竄が困難な時計である。シグネチャ・データの生成 1 0 4 は、映画フィルムへ電子透かし情報として埋め込み、映画フィルムを特定するためのシグネチャ・データをセキュア・タイマ 1 0 3 の時刻情報に基づいて生成する装置である。フィルムWMエンベッタ 1 0 5 は、映画フィルムへの電子透かし情報の埋め込み装置である。フィルムのマスターそのものに埋め込む方法と、マスターからの転写時に埋め込む方法がある。タイマ較正 1 0 6 は、再生装置に内蔵するセキュア・タイマの時刻を較正する仕組みを備える。
- 15

- ディスク・ユニーク・ナンバの発行 2 7 は、量産枚数の発行 1 3 の発行者から発行されたディスクの量産枚数に応じて、量産するディスクへ
- 20 記録されるディスク・ユニーク・ナンバを発行する。ディスク・ユニーク・ナンバは、全タイトルを通じたシリアル番号等からスクランブルされて得られるディスク毎に固有のランダムな番号とその検証値から構成される。検証値は、M D C (Message Digest Code)、あるいは、G U I D を鍵とした M A C (Message Authentication Code) などにより計算される。ディスク・ユニーク・ナンバは、一連のディスク毎に各ディスクを一意に識別するディスク識別番号として利用される。
- 25

第14図は、デジタル・ビデオ・ディスク60内のデータ記録領域の構成の一例を示す。フィジカル・インデックス記録領域61は、フィジカル・インデックスを記録するための領域である。フィジカル・インデックスは、本来のデータ読み出しに影響せずに多重して記録される。この記録方法では、本来のデータをディスク全領域に渡り読み出して、これをコピーしても、多重部分のフィジカル・インデックスがコピーされないことから、まるごとコピー（ビットバイビットコピー）に効果的とされる。

バースト・カッティング・エリアであるBCA62には、タイトルを特定するためのGUIDとディスクごとに異なる値となるディスク・ユニーク・ナンバーが記録される。BCAは、データ記録された後でディスクメディアに記録される。フィジカル・インデックスおよびBCAの具体的な記録方法は、上述した第1の実施形態において説明したのでここでは説明を省略する。

デバイス・リボケーション・リスト、ディスク・リボケーション・リスト、ディスク・キーは、ビデオコンテンツの記録される領域とは区別された領域、例えばリードインエリア63に書き換え不可能な状態で記録される。

データエリア64は、GUIDのハッシュ値が電子透かし情報として埋め込まれた暗号化されたビデオコンテンツを記録するデータ領域である。

第15図は、デジタル・ビデオ・ディスク60を再生するデジタル・ビデオ・ディスク再生装置70内の構成の一例を示す。ROM識別器72は、デジタル・ビデオ・ディスク再生装置70へ装着されたディスクが読み出し専用のデジタル・ビデオ・ディスク60であるか否かを判定するための識別を行う。もし、読み出し専用のデジタル・ビデオ・ディ

スク 6 0 であると判定されたならばスイッチ S W 1 をオン状態に設定する。そうでなければ、オフ状態に設定する。

デクリプタ 7 3 は、暗号化されたビデオコンテンツの復号を行う。暗号化検出器 7 4 は、デジタル・ビデオ・ディスク再生装置 7 0 がリポー
5 クされていないかどうかの確認とデジタル・ビデオ・ディスク 6 0 へ記録されたビデオコンテンツが暗号化記録されているかどうかの検査を行う。再生装置がリポークされておらずビデオコンテンツが暗号化記録されていたならば、スイッチ S W 2 をオン状態に設定する。そうでなければ、オフ状態に設定する。

10 M P E G 2 デコーダ 7 5 , 9 2 は、ビデオ圧縮を解き、ベースバンド・ビデオ信号へ変換する。ビデオ W M 検出器 7 6 は、ビデオコンテンツに埋め込まれたビデオ電子透かし情報を検出する。電子透かし情報の検出後、B C A 6 2 に記録される G U I D のハッシュ値を計算し、このハッシュ値と電子透かし情報を比較する。両者が一致しないことを確
15 認したのならば、スイッチ S W 3 をオフ状態に設定する。両者が一致した場合、または電子透かし情報が未検出の間は、スイッチ S W 3 はオン状態に設定される。

ディスク・リボケーション・チェッカー 7 7 は、B C A 6 2 に記録されたディスク・ユニーク・ナンバと、再生装置内の不揮発性メモリに記憶されたディスク・リボケーション・リスト内に登録された値とを比較
20 し、同じ値が登録されているか確認する工程である。もし、値が一致したならば、デジタル・ビデオ・ディスク 6 0 は、リボケーションの対象と判定してスイッチ S W 4 をオフ状態に設定する。値の一致が確認されない間は、オン状態に設定される。

25 不揮発性メモリ 7 9 は、再生装置が再生したメディアの記録として、ディスク・ユニーク・ナンバを記憶するための不揮発性メモリである。

管理機構 20 とデジタル・ビデオ・ディスク再生装置 70 とのネットワーク接続が成立しているときに、この不揮発性メモリ 79 内の再生メディア記録データをデバイス ID 89、デバイス・シリアル・ナンバ 91 とともに管理機構 20 へ転送し、転送後にこの不揮発性メモリ 79 内の
5 データを消去して空き領域を確保する。ネットワーク接続においては、SSL 認証、IPsec 暗号化に基づく VPN などの暗号化通信が行われることなどが想定される。

バージョン・チェッカー 80 は、デジタル・ビデオ・ディスク 60 に記録されるディスク・リボケーション・リストを不揮発性メモリ 81 へ
10 格納する際に、既に格納されているディスク・リボケーション・リストのバージョンとデジタル・ビデオ・ディスク 60 に記録されているディスク・リボケーション・リストのバージョンとどちらが新しいバージョンであるかの比較を行う。もし、デジタル・ビデオ・ディスク 60 に記録されたデータのバージョンの方が新しいのであれば、スイッチ SW 6
15 をオン状態に設定して不揮発性メモリ 81 内のディスク・リボケーション・リストのデータを更新する。

不揮発性メモリ 81 は、ディスク・リボケーション・リストを格納するための不揮発性メモリである。ディスク・リボケーション・リストは、管理機構 20 とデジタル・ビデオ・ディスク再生装置 70 とのネットワーク
20 接続が確立している状態において、管理機構 20 から転送される場合もあり、この時もメディアから更新されるのと同じプロセスで不揮発性メモリ 81 内のデータの更新が行われる。

セキュア・タイマ 82 は、デジタル・ビデオ・ディスク再生装置 70 に内蔵される改竄が困難なタイマである。出力する時刻情報をもとにシ
25 グネチャ・データが生成される。タイマの時刻情報は管理機構 20 とデジタル・ビデオ・ディスク再生装置 70 とのネットワーク接続が確立し

ている状態において、管理機構 20 内のセキュア・タイマ 103 との同期がとられ較正される場合もある。

シグネチャ・リスト生成器 83 は、セキュア・タイマ 82 の出力する時刻情報より遡って複数分の、例えば 100 タイトル分の映画フィルムのシグネチャ・データを生成してシグネチャ・リストを作成する。この
5 100 タイトルは例えば上映中の新作の映画であり、まだデジタル・ビデオ・ディスク 60 として量産・販売されていないタイトルである。もし、再生装置がこれを再生したとしたら、それは不正に流出したコンテンツであるとみなされる。

10 フィルムWM検出器 84 は、再生中のビデオコンテンツに電子透かし情報として埋め込まれたフィルム電子透かしステータスを検出する工程である。

比較器 88 は、フィルムWM検出器 84 で検出されたフィルム電子透かしステータスとシグネチャ・リスト生成器 83 内に格納された不正に
15 流出したコンテンツであることを特定するためのシグネチャ・リストとを比較する工程である。フィルムWM検出器 84 の検出が完了していない間は、スイッチ SW5 はオン状態に設定される。フィルムWM検出器 84 の検出が完了し、かつそのステータスがシグネチャ・リスト生成器 83 に格納されたシグネチャ・リストに登録済みであれば、再生コンテ
20 ンツは不正に流出したコンテンツであるとみなし、スイッチ SW5 をオフ状態に設定することでコンテンツの再生動作を中断する。あるいは、不正なコンテンツを再生していることを示すメッセージを再生画面へスーパーインポーズして、利用者へ告知する。

デバイス ID 89 は、デジタル・ビデオ・ディスク再生装置 70 の識別
25 別データである。再生装置の製造業者単位、あるいは機種単位で、固有の識別番号が配布される。

デバイス・キー 90 は、デバイス ID 89 とディスク・リボケーション・リストから計算されるデータと組み合わせることでデジタル・ビデオ・ディスク 60 へ記録された暗号化等により秘匿されたディスク・キーを導出する。

- 5 デバイス・シリアル・ナンバ 91 は、デジタル・ビデオ・ディスク再生装置 70 の製造業者によって配布される一連のデバイス毎にデバイスを特定するための製造シリアル番号である。

- 10 スイッチ SW1 は、ROM 識別器 72 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW2 は、暗号化検出器 74 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW3 は、ビデオ WM 検出器 76 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW4 は、ディスク・リボケーション・チェッカー 77 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW5 は、比較器 88 の判定結果に基づいてビデオコンテンツ再生を制御するためのスイッチである。スイッチ SW6 は、バージョン・チェッカー 80 の判定結果に基づいてディスク・リボケーション・リストの格納を制御するためのスイッチである。

< 1. 編集制作工程の説明 >

- 20 第 16 図は、デジタル・ビデオ・ディスク 60 の編集制作工程の流れを示す。第 16 図に示すデジタル・ビデオ・ディスク 60 の編集制作工程の処理フローをもとに、第 11 図～第 13 図の全体システム構成を示すブロック図を参照しながら説明する。

- 25 コンテンツ所有者 10 よりデジタル・ビデオ・ディスク化を希望するビデオコンテンツを受け取ることで編集制作プロジェクトが発生する。デジタル・ビデオ・ディスク制作のための編集制作プロジェクトが起こ

ると、編集制作工程 30 は管理機構 20 に対して GUID の発行を要請する（ステップ S 2 1 1）。なお、図中の CA は、管理機構 20 を示す。

この要請を受けた管理機構 20 はタイトルごとに固有の GUID を
5 発行する（ステップ S 2 1 2）。GUID の発行を受けた編集制作工程 30 はステップ S 2 1 4 においてビデオコンテンツへ GUID のハッシュ値を埋め込む（ステップ S 2 1 3）。

管理機構 20 とのライセンス契約に基づいて提供を受けたビデオ WM
エンベッタ 31 では、GUID のハッシュ値を計算した上で、そのハ
10 ッシュ値を電子透かし情報としてビデオコンテンツのビデオ信号へ埋め込む（ステップ S 2 1 4）。

ステップ S 2 1 0、すなわち、ステップ S 2 1 1 からステップ S 2 1
4 において、編集制作工程 30 と管理機構 20 とは SSL、IPsec
技術などを利用した VPN を構成するものとし、セキュアなネットワー
15 ク接続によるデータの送受信が可能な状態にあるものとする。

ハッシュ値を電子透かし情報として埋め込んであるビデオ信号とともに、ビデオコンテンツ内のオーディオ信号、字幕などのサブタイトル、ビデオコンテンツのアクセスを容易とするためのメニュー、およびインタラクティブ機能を実現するためのデータやプログラムをエンコードす
20 る（ステップ S 2 1 5）。

各ファイル・データを多重化し、ファイルシステム管理情報であるボリューム・デスクリプタの中に GUID を記録する（ステップ S 2 1
6）。ディスク製造工程へ作業を引き継ぐために、HD-DVD ディスク・イメージをマスタフォーマットへ書き込む（ステップ S 2 1 7）。

25 < 2. ディスク製造工程の説明 >

第 17 図は、デジタル・ビデオ・ディスク 60 の製造工程の流れを示

す。第17図に示すデジタル・ビデオ・ディスク60の製造工程の処理フローをもとに、第11図～第13図の全体システム構成を示すブロック図と、第14図のディスクメディア関係図を参照しながら説明する。

HD-DVDディスク・イメージを編集制作工程30から受け取る
5 (ステップS221)。ボリューム・デスクリプタを展開してGUID
Dを読み出す。ここで得られたGUIDをディスク製造工場から管理機構20へ転送する(ステップS222)。

コンテンツ所有者10は編集制作工程30に対する編集制作用ビデオ
コンテンツを渡すとともにディスク製造工場に対してディスク量産の発
10 注を実施しており、その際に発注枚数も指定される(ステップS22
3)。

コンテンツ所有者10からディスク量産の発注を受けたディスク製造
工場は、GUIDと発注枚数を管理機構20へ転送し、製造するディ
スク1枚1枚に書き込むディスク・ユニーク・ナンバの発行を要求する
15 (ステップS224)。

管理機構20ではディスク製造工場から受け取ったGUIDから、
ビデオコンテンツのタイトルを特定する。また、受け取った発注枚数か
ら製造するディスクメディアが全タイトルにわたって1枚1枚が固有の
ランダムな番号とその検証値から構成される未使用のディスク・ユニ
20 ク・ナンバを受注枚数分だけ厳正に算出する(ステップS225)。検
証値は、例えばMDC、あるいは、GUIDを鍵としたMACなどの方
法により計算されるものとする。

管理機構20はディスク製造工場に対して、ディスク製造の許諾すな
わちHD-DVDディスク・イメージを暗号化するために必要なディス
ク・キー、ディスク・ユニーク・ナンバー式、デバイス・リボケーショ
25 ン・リスト、ディスク・リボケーション・リストを転送する(ステップ

S 2 2 6)。デバイス・リボケーション・リストは不正に製造されたディスク再生装置において正規ディスクメディアの再生が制限されるようにするためのデータである。ディスク・リボケーション・リストは不正に製造されたディスクメディアを正規のディスク再生装置において再生
5 が制限されるようにするためのデータである。

ディスク製造工場は、編集制作工程 3 0 から受け取った H D - D V D ディスク・イメージに、管理機構 2 0 から受け取ったこれらのデータを組み合わせ、さらに管理機構 2 0 とのライセンス契約に基づいて提供された暗号化技術を利用して H D - D V D ディスク・イメージを暗号化し
10 てディスク・マスター（原盤）を作成する（ステップ S 2 2 7）。

ステップ S 2 2 0、すなわち、ステップ S 2 2 4 からステップ S 2 2 7 において、ディスク製造工場と管理機構 2 0 とは S S L、I P s e c 技術などを利用した V P N を構成するものとし、セキュアなネットワーク接続によるデータの送受信が可能な状態にあるものとする。

15 ディスク・マスター（原盤）からディスクメディアを大量生産する（ステップ S 2 2 8）。製造されたディスクメディアへ B C A を焼きこむ。B C A には、タイトルを特定できる G U I D と 1 枚 1 枚が異なる値を持つディスク・ユニーク・ナンバが記録される（ステップ S 2 2 9）。

20 < 3. ディスク再生装置の説明 >

第 1 8 図および第 1 9 図は、デジタル・ビデオ・ディスク 6 0 の再生装置における処理の流れを示す。作図スペースの制約によって、処理の流れを第 1 8 図および第 1 9 図に分割している。第 1 8 図および第 1 9 図に示すデジタル・ビデオ・ディスク 6 0 の再生装置の処理フローをも
25 とに、第 1 5 図の、デジタル・ビデオ・ディスク再生装置 7 0 の構成を示すブロック図を参照しながら、ディスクメディアが再生装置へ装着さ

れた後の再生装置の動作を説明する。

まず、再生装置は、装着されたディスクメディアからフィジカル・インデックス記録領域 61 を読み出す（ステップ S 230）。フィジカル・インデックス記録領域 61 の読み出し方法は再生装置および再生装置に利用される部品の製造業者が管理機構 20 と正規の契約を結ぶことにより提供される。

読み出しにより、フィジカル・インデックスが正しく検出されるかどうかを判定する（ステップ S 231）。再生装置が正しくフィジカル・インデックスを検出できなかった場合、この第 2 の実施形態で述べる暗号化方式でコンテンツが暗号化された再生専用ディスクメディア以外のディスク・メディアであると判断し、後述するフィルム WM チェックへ処理が移行する。ここで、再生装置は再生専用ディスクメディアのみを再生するものとした場合、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝えることも想定される。

再生装置が正しくフィジカル・インデックスを検出した場合、BCA データを読み、GUID とディスク・ユニーク・ナンバを取得する（ステップ S 232）。そして、取得したディスク・ユニーク・ナンバの正当性を検証値により確認する（ステップ S 233）。正当性が確認されなければ、不正に製造されたディスクメディアと判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。正当性が確認されれば、ステップ S 234 へ進む。

ディスク・ユニーク・ナンバと同一の値を持つ再生専用ディスクメディアを過去に再生したことがあるかどうかを調べるため、不揮発性メモリ 79 に記憶されている再生ディスク・メディア・リストを検索する（ステップ S 234）。

再生ディスク・メディア・リスト内に同じ値が存在すればステップ S

236へ進む。再生ディスク・メディア・リスト内に同じ値が存在しなければ、その値を不揮発性メモリ79へ格納する（ステップS235）。このリストは、デジタル・ビデオ・ディスク再生装置70と管理機構20とがセキュアにネットワーク接続されているときにデジタル・ビデオ・ディスク再生装置70から管理機構20へ転送され、メモリの空き状況に応じて、転送後に不揮発性メモリ79に記録されたリストは消去される。

ディスク・ユニーク・ナンバの値で、不揮発性メモリ81に記憶されているディスク・リボケーション・リストを検索する（ステップS236）。ディスク・リボケーション・リスト内に同一の値が存在すれば、再生ディスクメディアはリボケーションの対象と判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。

ディスク・リボケーション・リスト内に同一の値が存在しなければ、リードイン領域のデバイス・リボケーション・リストとディスク・リボケーション・リストと暗号化等により秘匿されたディスク・キーとを読み出す（ステップS237）。これらの情報はディスクに記録された暗号化ビデオコンテンツを復号するために必要とされる。この暗号化ビデオコンテンツの復号技術は再生装置および再生装置に利用される部品の製造業者が管理機構20と正規の契約を結ぶことにより提供される。

デバイス・リボケーション・リストとディスク・リボケーション・リストと暗号化等により秘匿されたディスク・キーが正しく読み出せたかどうかを判定する（ステップS238）。デバイス・リボケーション・リスト、ディスク・リボケーション・リストあるいは暗号化等により秘匿されたディスク・キーを正しく読み出すことが出来なかった場合など、ビデオコンテンツが適正に暗号化記録されていないと判断される場合には、この第2の実施形態で述べる暗号化方式でコンテンツが暗号化され

た再生専用ディスクメディア以外のディスク・メディアであると判断し、後述するフィルムWMチェックへ処理が移行する。なお、著作権保護技術の運用方法の一つとして、ここで再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝えるという手段をとることも

5 ありえる。

デバイス・リボケーション・リスト、ディスク・リボケーション・リストおよび暗号化等により秘匿されたディスク・キーを正しく読み出すことが出来た場合には、ディスク・リボケーション・リストの更新を行う（ステップS 2 3 9）。このリストにはバージョン情報が含まれている。不揮発性メモリ 8 1 内に記憶されている過去のディスク・リボケーション・リストのバージョンよりも新しいディスク・リボケーション・リストを取得した場合には、不揮発性メモリ 8 1 内のリストを更新する。メモリ内には複数のバージョンのディスク・リボケーション・リストを記憶させ、古いバージョンのデータから順番に消去するというF I F O

10 構造をとることもありうる。データ領域を読み出し、復号された暗号化ビデオコンテンツの再生を開始する（ステップS 2 4 0）。

再生開始後、ある時間が経過するまでビデオ信号に埋め込まれているビデオ電子透かしが検出されるのを待つ（ステップS 2 4 1）。ある一定時間が経過しても、または、ある一定量のストリームを処理してもビデオ電子透かしが検出されなかった場合、再生ディスクメディアは不正な編集制作工程によってつくられたビデオコンテンツであると判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。このビデオ電子透かしの検出技術は再生装置および再生装置に利用される部品の製造業者が管理機構 2 0 と正規の契約を結ぶこと

20 により提供される。

ある一定時間内に、もしくは、ある一定処理量内でビデオ電子透かし

が検出されたならば、その電子透かし情報が GUID のハッシュ値と同じ値を示すか否かを確認する（ステップ S 2 4 2）。一致しなかった場合、再生ディスクメディアは不正な編集制作工程によってつくられたビデオコンテンツである、あるいは不正な製造工程で製造されたディスク・メディアであると判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。一致した場合には、再生動作を継続する。

この第 2 の実施形態で述べる暗号化方式でコンテンツが暗号化された再生専用ディスクメディア以外のディスク・メディアであると判断した場合、即ちコンテンツが暗号化されていない再生専用ディスクメディアや記録型ディスクメディアに記録されたビデオコンテンツや DVD・SVCD などの異なるフォーマットのディスクメディアに記録されたビデオコンテンツを再生する場合、再生しながらフィルム WM の検出をして違法なコンテンツであるか否かの判定を行う。そのときの処理の流れを第 2 0 図に示す。

第 2 0 図に示すフィルム WM チェックの処理は、ビデオコンテンツの再生中に、シグネチャ・リスト生成器 8 3 内にシグネチャ・リストを生成する（ステップ S 2 4 3）。シグネチャ・リストはコンテンツ所有者 1 0 が劇場で新作の映画を公開する際に、その新作映画がディスクメディアとして販売される以前に海賊行為により製造されたディスクメディアが販売されることで、新作映画の興行収入を獲得する機会と正規ディスクメディアの販売収入を獲得する機会を損なうことを防ぐことを目的として設けられたものであり、興行中もしくは興行予定の映画を特定するためシグネチャ・データが複数記録されたデータベースである。このシグネチャ・リストの生成方法は再生装置および再生装置に利用される部品の製造業者が管理機構 2 0 と正規の契約を結ぶことにより提供され

る。

- フィルムWM検出器 8 4 によるフィルム電子透かしの検出が実行される。フィルム電子透かしが検出されたならば、そのステータスでシグネチャ・リスト生成器 8 3 内に格納されているシグネチャ・リストを検索
- 5 し一致したシグネチャ・データが登録されているか確認する（ステップ S 2 4 4）。もし登録されていることが確認されたならば、再生ディスクメディアは劇場で上映された作品を不正に取得し、これをソースとして編集制作・製造されたビデオコンテンツであると判断され、再生動作を停止しユーザインターフェースを通じて停止したことをユーザへ伝える。
- 10 登録が無ければ正規の契約に基づいて編集制作・製造されたディスク・メディアであることが確認され、通常の再生動作が保証される。このフィルム電子透かしの検出技術は再生装置および再生装置に利用される部品の製造業者が管理機構 2 0 と正規の契約を結ぶことにより提供される。
- 15 以上説明したこの発明の第 2 の実施形態では、デジタル・ビデオ・ディスク 6 0 に G U I D と G U I D のハッシュ値とが、異なる 2 種類の記録方法で記録される。G U I D は、ディスクメディアの B C A に記録される。G U I D のハッシュ値は、デジタル・ビデオ・ディスク化を行うビデオコンテンツに電子透かし情報として埋め込まれる。デジタル・ビデオ・ディスク再生装置 7 0 は、B C A から G U I D を読み取り、読み
- 20 取った G U I D のハッシュ値と、ビデオコンテンツに埋め込まれた電子透かし情報とを比較して、一致したら再生動作を行う。これにより、管理機構 2 0 の認可を受けた編集制作工程 3 0 でビデオ編集されたコンテンツが、同じく管理機構 2 0 の認可を受けたディスク製造工程（マスタリング工程 4 0、ディスク量産工程 5 0）で製造されたデジタル・ビデオ・ディスク 6 0 へ記録されたことを、デジタル・ビデオ・ディスク再
- 25

生装置 70 が確認できる。

したがって、不正に入手したビデオ信号を、不正な編集制作工程でビデオ編集し、ディスク製造工場で製造し配布されたディスクメディアをデジタル・ビデオ・ディスク再生装置 70 が識別可能であり、これに対して再生制限を加えることが可能となる。

また、この発明の第 2 の実施形態では、電子透かし情報として埋め込まれた GUID の情報が正しく検出され、ディスクメディアの BCA へ別途記録済みの GUID の情報と比較し、一致が確認されたことを持って再生許可されるのであるから、電子透かし情報を検出不可能とするための攻撃は全く意味をなさない。したがって、電子透かし技術に対する攻撃への対処が不要であり、適用する電子透かし技術が簡易なものとなる。このことは、新技術を適用する再生装置の低コスト化に貢献する。

また、この発明の第 2 の実施形態では、マスタリング工程 40 において、管理機構 20 から発行されたフィジカル・インデックスがデジタル・ビデオ・ディスク 60 に記録される。このフィジカル・インデックスは、再生専用ディスクメディアに本来のデータ読み出しに影響せずに多重記録されている。デジタル・ビデオ・ディスク再生装置 70 は、再生したディスクからフィジカル・インデックスが検出された場合に再生動作を行うように構成されている。これにより、管理機構 20 の認可を受けたディスク製造工場で製造された再生専用ディスク・メディアであるか否かを、デジタル・ビデオ・ディスク再生装置 70 が確認することを可能とする。

また、デジタル・ビデオ・ディスク 60 に記録されたビデオコンテンツは暗号化されている。これにより、デジタル・ビデオ・ディスク再生装置 70 は、不正に入手したビデオ信号を、不正なディスク製造工場で製造し配布されたディスク・メディアであるか否かを、ROM 識別器 7

2でのフィジカル・インデックスの検出による再生専用ディスク・メディアであるかの確認と、暗号化検出器74によるデジタル・ビデオ・ディスク60のビデオコンテンツが暗号化記録されたものであるかの確認との2つの手段で識別可能であり、これに対して再生制限を加えることが可能となる。

また、この発明の第2の実施形態では、指定された枚数以上のディスクを余分に製造しようとする、ディスク・ユニーク・ナンバの中のランダムな固有の番号が必ず重複することになる。この重複は、デジタル・ビデオ・ディスク再生装置70とネットワーク接続される管理機構20の管理サーバ等により監視することで、検出が可能である。したがって、管理機構20の認可を受けたディスク製造工場において、正規に発注された枚数を超えたディスク製造が行われないように管理することが可能となる。さらにディスク毎にランダムな値のディスク・ユニーク・ナンバを利用することで、ネットワークへこのデータを流してもディスク・ユニーク・ナンバからタイトルを特定することができず、利用者のプライバシーを保護することが可能となる。

また、この発明の第2の実施形態では、映画館等で上映されるフィルムコンテンツには、フィルムWMエンベッタ105においてシグネチャ・データが電子透かしにより埋め込まれている。デジタル・ビデオ・ディスク再生装置70は、ディスクの再生の際、シグネチャ・リスト生成器83において時間情報をもとにシグネチャ・リストを生成し、フィルムWM検出器84においてフィルムコンテンツに埋め込まれた電子透かし情報を読み取る。そして比較器88において、シグネチャ・リストとシグネチャ・データとを比較し、両者が一致した場合には、再生を停止する。これにより、再生したディスクメディアが新作上映中の映画館から不正に流出されたビデオ信号から製造された海賊版ディスク・メディア

ィアであるか否かをデジタル・ビデオ・ディスク再生装置 70 は確認することが可能となり、これに対して再生制限を加えることが可能となる。

第 2 の実施形態によるシグネチャ・リスト、シグネチャ・データを利用した再生制限の具体的な例については、上述した第 1 の実施形態における第 10 図を参照した説明と同様であるので、その説明は省略する。

この発明は、上述したこの発明の実施形態に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば、上述した第 1 および第 2 の実施形態では、GUID をタイトル毎に割り振るとしたが、これに限らず、タイトルが特定できるならば、デジタル・ビデオ・ディスクの製造依頼毎など他の割り振り方であっても良い。

また、上述した第 1 および第 2 の実施形態では、GUID を BCA に記録し、GUID のハッシュ値をビデオコンテンツの電子透かし情報として記録したが、電子透かし情報の値と BCA の値の真正性が保証されればよいので、GUID をビデオコンテンツの電子透かし情報として記録し、GUID のハッシュ値を BCA に記録するなど、他の組み合わせであっても良い。

また、上述した第 1 および第 2 の実施形態におけるフィジカル・インデックスは、データ領域上の一部に多重記録されるように図示されているが、これに限らず、データ領域の全面や、リードインエリア等に多重記録しても良い。また、上述した第 1 および第 2 の実施形態では、電子透かしを埋め込んだビデオコンテンツを記録してから、BCA に GUID 等を記録しているが、記録の順番はこれに限定されるものではない。

また、上述した第 1 および第 2 の実施形態のリポケーション・リストやディスク・キーは、レプリケータによる製造工程前に、リードイン領域に記録するとしたが、これに限らず、例えばデータ量が多いときなど

は、データ領域に暗号化して記録しても良い。

また、上述した第1の実施形態では、再生装置がセキュア・タイマを持っているとしたが、セキュア・タイマを持たず、著作権管理サーバ等の外部のセキュア・タイマの時間情報を参照するようにしても良い。

- 5 また、上述した第1および第2の実施形態では、グローバル・シリアル・ナンバまたはディスク・ユニーク・ナンバによる判定を行ってから、シグネチャ・リストによる判定を行っているが、これら判定の順番は、これに限ったものではない。

- 10 また、上述した第1および第2の実施形態では、ビデオコンテンツの記録媒体として光ディスクを用いて説明したが、これに限らず、磁気ディスク、光磁気ディスク、光カード、メモリカードなど、他の再生専用の記録媒体に適用することもできる。

- 15 以上詳細に説明したように、この発明によれば、正規の記録媒体であるか否かを判定可能な情報を記録媒体に記録することで、再生装置が記録媒体を再生する際、記録媒体から判定可能な情報を読み取り、読み取った情報を基に正規でない記録媒体の再生を制限することができる。したがって、ビデオコンテンツの不正な複製行為から著作権者の利益を守ることができる。

20

25

請 求 の 範 囲

1. ビデオコンテンツのデータが記録されている記録媒体であって、
前記ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル情報の真正性の保証に必要となるタイトルメッセージが、前記ビデオコンテンツのデータに電子透かし情報として埋め込まれ、
前記タイトル情報または前記タイトルメッセージが、前記データの記録されている領域と異なる記録領域に記録される記録媒体。
2. 前記タイトルメッセージが、前記タイトル情報から一方向性の関数により得られる請求の範囲第1項に記載の記録媒体。
- 10 3. ビデオコンテンツのデータが記録された記録媒体が製造される記録媒体製造方法であって、
前記ビデオコンテンツのデータを編集する編集ステップと、
前記ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル情報の真正性の保証に必要となるタイトルメッセージを、前記ビデオコンテンツのデータに電子透かし情報として埋め込む第一のタイトル記録ステップと、
前記タイトル情報または前記タイトルメッセージが、前記データの記録されている領域と異なる記録領域に記録される第二のタイトル記録ステップとを有する記録媒体製造方法。
- 20 4. 前記タイトルメッセージが、前記タイトル情報から一方向性の関数により得られる請求の範囲第3項に記載の記録媒体製造方法。
5. 前記タイトル情報がネットワークを介して接続した著作権管理サーバから提供されるタイトル情報提供ステップを有する請求の範囲第3項に記載の記録媒体製造方法。
- 25 6. ビデオコンテンツのデータが記録され、当該ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル情報の真正性の保証に必

要となるタイトルメッセージが前記ビデオコンテンツのデータに電子透かし情報として埋め込まれ、前記タイトル情報または前記タイトルメッセージが前記データの記録されている領域と異なる記録領域に記録された記録媒体を再生する再生方法であって、

- 5 前記データの記録されている領域と異なる記録領域に記録されているタイトル情報またはタイトルメッセージを検出する第一のタイトル情報検出ステップと、

前記電子透かし情報として埋め込まれているタイトル情報またはタイトルメッセージを検出する第二のタイトル情報検出ステップと、

- 10 前記第一及び第二のタイトル情報検出ステップでそれぞれ検出されたタイトル情報またはタイトルメッセージの真正性が保証されるか否かを判定する判定ステップと、

前記判定ステップで真正性が保証されなかった場合には前記記録媒体の再生動作を制限する再生制限ステップとを有する再生方法。

- 15 7. ビデオコンテンツのデータが記録され、当該ビデオコンテンツのタイトルを示すタイトル情報または当該タイトル情報の真正性の保証に必要なタイトルメッセージが前記ビデオコンテンツのデータに電子透かし情報として埋め込まれ、前記タイトル情報または前記タイトルメッセージが前記データの記録されている領域と異なる記録領域に記録された記録媒体を再生する再生装置であって、

20 前記データの記録されている領域と異なる記録領域に記録されているタイトル情報またはタイトルメッセージを検出する第一のタイトル情報検出部と、

- 25 前記電子透かし情報として埋め込まれているタイトル情報またはタイトルメッセージを検出する第二のタイトル情報検出部と、

前記第一及び第二のタイトル情報検出部でそれぞれ検出されたタイト

ル情報またはタイトルメッセージの真正性が保証されるか否かを判定する判定部と、

前記判定部で真正性が保証されなかった場合には前記記録媒体の再生動作を制限する制御部とを有する再生装置。

- 5 8. ビデオコンテンツのデータが記録されている記録媒体であって、
一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報と、
リボークすべき記録媒体を、少なくとも前記媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストとが記録されている記録媒体。

- 10 9. 前記識別メッセージが、前記媒体識別情報から一方向性の関数により得られる請求の範囲第8項に記載の記録媒体。

10. 前記媒体識別情報が、一連の記録媒体毎に連続性を有し、かつ記録媒体毎に固有であり、

- 15 前記媒体リボケーション・リストが、リボークすべき記録媒体を指示するのに前記ビデオコンテンツのタイトル情報と前記識別メッセージとを用いる請求の範囲第8項に記載の記録媒体。

11. 前記媒体識別情報が、一連の記録媒体毎に連続性を有しないで、かつ記録媒体毎に固有であり、

- 20 前記媒体リボケーション・リストが、リボークすべき記録媒体を指示するのに当該媒体識別情報を用いる請求の範囲第8項に記載の記録媒体。

12. 前記媒体リボケーション・リストが、バージョン情報を有している請求の範囲第8項に記載の記録媒体。

13. 不正な機器をリボークするためのデバイス・リボケーション・リストも記録されている請求の範囲第8項に記載の記録媒体。

- 25 14. ビデオコンテンツのデータが記録された記録媒体が製造される記録媒体製造方法であって、

前記ビデオコンテンツのデータを編集する編集ステップと、

リボークすべき記録媒体を、少なくとも一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストを記録する媒体リスト記録ステップと、

各媒体毎の媒体識別情報が前記ビデオコンテンツのデータが記録された領域の記録方法と異なる方法で記録する識別情報記録ステップとを有する記録媒体製造方法。

15 15. 前記識別メッセージは、前記媒体識別情報から一方向性の関数により得られる請求の範囲第14項に記載の記録媒体製造方法。

16. 前記媒体識別情報が、一連の記録媒体毎に連続性を有し、かつ記録媒体毎に固有であり、

15 前記媒体リボケーション・リストが、リボークすべき記録媒体を指示するのに前記ビデオコンテンツのタイトル情報と前記識別メッセージとを用いる請求の範囲第14項に記載の記録媒体製造方法。

17. 前記媒体識別情報が、一連の記録媒体毎に連続性を有しないで、かつ記録媒体毎に固有であり、

20 前記媒体リボケーション・リストが、リボークすべき記録媒体を指示するのに当該媒体識別情報を用いる請求の範囲第14項に記載の記録媒体製造方法。

18. 前記媒体リボケーション・リストが、バージョン情報を有している請求の範囲第14項に記載の記録媒体製造方法。

25 19. 前記記録媒体に不正な機器をリボークするためのデバイス・リボケーション・リストも記録されている請求の範囲第14項に記載の記録媒体製造方法。

20. ビデオコンテンツのデータが記録され、一連の記録媒体毎に各記

録媒体を一意に識別する媒体識別情報と、リボークすべき記録媒体を、少なくとも前記媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストとが記録されている記録媒体を再生する再生方法であって、

- 5 前記媒体識別情報を読み出す媒体識別情報読み出しステップと、
 前記媒体リボケーション・リストを読み出す媒体リスト読み出しステップと、

 読み出した前記媒体識別情報または当該媒体識別情報の識別メッセージをメモリに蓄積する媒体識別情報蓄積ステップと、

- 10 蓄積された前記媒体識別情報または前記識別メッセージが前記媒体リボケーション・リストに含まれているか否かを判定する媒体リスト判定ステップと、

 前記媒体リスト判定ステップでリボークすべきと判断された場合には前記記録媒体の再生動作を制限する再生制限ステップとを有する再生方

- 15 法。

 2 1. 前記媒体リボケーション・リストが、バージョン情報を有している請求の範囲第 2 0 項に記載の再生方法。

 2 2. 前記媒体リボケーション・リストが、再生動作を制限する機器とネットワークを介して接続した著作権管理サーバから更新される、媒体

- 20 リスト更新ステップを有する請求の範囲第 2 1 項に記載の再生方法。

 2 3. 前記記録媒体に不正な機器をリボークするためのデバイス・リボケーション・リストが記録されているとともに、

 当該デバイス・リボケーション・リストを読み出すデバイスリスト読み出しステップと、

- 25 読み出した当該デバイス・リボケーション・リストを蓄積するデバイスリスト蓄積ステップと、

- 再生している機器が蓄積した当該デバイス・リボケーション・リストに含まれているか否かを判定するデバイスリスト判定ステップとを有し、
- 前記デバイスリスト判定ステップでリボークすべきと判断された場合には前記記録媒体の再生動作を制限する再生制限ステップとを有する請求の範囲第20項に記載の再生方法。
24. 前記デバイス・リボケーション・リストが、再生動作を制限する機器とネットワークを介して接続した著作権管理サーバから更新されるデバイスリスト更新ステップを有する請求の範囲第23項に記載の再生方法。
- 10 25. ビデオコンテンツのデータが記録され、一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報が記録されている記録媒体を再生する再生方法であって、
- 前記媒体識別情報を読み出す媒体識別情報読み出しステップと、
- 読み出した前記媒体識別情報または当該媒体識別情報の識別メッセージをメモリに蓄積する媒体識別情報蓄積部と、
- 15 著作権管理サーバとネットワークを介して接続し、当該著作権管理サーバからリボークすべき記録媒体を前記媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストを受信し、蓄積した前記媒体識別情報または当該媒体識別情報の識別メッセージが前記媒体リボケーション・リストに含まれているか否かを判定する媒体リスト判定ステップとを有し、
- 20 前記判定ステップでリボークすべきと判断された場合には前記記録媒体の再生動作を制限する再生制限ステップとを有する再生方法。
26. 前記媒体リボケーション・リストが、バージョン情報を有している請求の範囲第25項に記載の再生方法。
- 25 27. 前記媒体リボケーション・リストが、前記著作権管理サーバから

更新される媒体リスト更新ステップを有する請求の範囲第 26 項に記載の再生方法。

28. 前記記録媒体に不正な機器をリボークするためのデバイス・リボケーション・リストが記録されているとともに、

- 5 当該デバイス・リボケーション・リストを読み出すデバイスリスト読み出しステップと、

再生している機器が読み出した当該デバイス・リボケーション・リストに含まれているか否かを判定するデバイスリスト判定ステップとを有し、

- 10 前記デバイスリスト判定ステップでリボークすべきと判断された場合には前記記録媒体の再生動作を制限する再生制限ステップとを有する請求の範囲第 25 項に記載の再生方法。

29. 前記デバイス・リボケーション・リストが、前記著作権管理サーバから更新されるデバイスリスト更新ステップを有する請求の範囲第 2

- 15 8 項に記載の再生方法。

30. ビデオコンテンツのデータが記録されている記録媒体を再生する再生装置であって、

- 一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報と、リボークすべき記録媒体を、少なくとも前記媒体識別情報または当該媒体
20 識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストとを読み出す読み出し部と、

読み出した前記媒体識別情報または当該媒体識別情報の識別メッセージを蓄積する媒体識別情報蓄積部と、

- 蓄積された前記媒体識別情報または前記識別メッセージが前記媒体リ
25 ボケーション・リストに含まれているか否かを判定する判定部と、

前記判定部でリボークすべきと判断された場合には前記記録媒体の再

生動作を制限する制御部とを有する再生装置。

3 1. 前記媒体リボケーション・リストが、バージョン情報を有している請求の範囲第 3 0 項に記載の再生装置。

3 2. 前記媒体リボケーション・リストが、再生動作を制限する機器と
5 ネットワークを介して接続した著作権管理サーバから更新される請求の
範囲第 3 1 項に記載の再生装置。

3 3. 前記記録媒体に不正な機器をリボークするためのデバイス・リボ
ケーション・リストが記録されているとともに、

10 当該デバイス・リボケーション・リストを読み出すデバイスリスト読
み出し部と、

読み出した当該デバイス・リボケーション・リストを蓄積するデバイ
スリスト蓄積部と、

再生している機器が蓄積した当該デバイス・リボケーション・リスト
に含まれているか否かを判定するデバイスリスト判定部と、

15 前記デバイスリスト判定部でリボークすべきと判断された場合には前
記記録媒体の再生動作を制限する制御部とを有する請求の範囲第 3 0 項
に記載の再生装置。

3 4. 前記デバイス・リボケーション・リストが、再生動作を制限する
機器とネットワークを介して接続した著作権管理サーバから更新される
20 請求の範囲第 3 3 項に記載の再生装置。

3 5. ビデオコンテンツのデータが記録されている記録媒体を再生する
再生装置であって、

一連の記録媒体毎に各記録媒体を一意に識別する媒体識別情報を読み
出す読み出し部と、

25 読み出した前記媒体識別情報または当該媒体識別情報の識別メッセ
ージを蓄積する媒体識別情報蓄積部と、

著作権管理サーバからリボークすべき記録媒体を前記媒体識別情報または当該媒体識別情報の真正性の保証に必要な識別メッセージで指示する媒体リボケーション・リストを受信する媒体リスト受信部と、

前記蓄積した媒体識別情報または識別メッセージが前記受信した媒体
5 リボケーション・リストに含まれているか否かを判定する媒体リスト判定部と、

前記媒体リスト判定部でリボークすべきと判断された場合には前記記録媒体の再生動作を制限する制御部とを有する再生装置。

36. 前記媒体リボケーション・リストが、バージョン情報を有している
10 請求の範囲第35項に記載の再生装置。

37. 前記受信した媒体リボケーション・リストが蓄積される媒体リスト蓄積部と、

前記著作権管理サーバが有する媒体リボケーション・リストのバージョン情報より前記蓄積された媒体リボケーション・リストのバージョン
15 情報が新しい場合に、前記蓄積された媒体リボケーション・リストが前記著作権管理サーバの媒体リボケーション・リストにより更新される請求の範囲第36項に記載の再生装置。

38. 前記記録媒体に不正な機器をリボークするためのデバイス・リボケーション・リストが記録されているとともに、

20 前記読み出し部が、当該デバイス・リボケーション・リストを読み出し、

再生している機器の情報が読み出した当該デバイス・リボケーション・リストに含まれているか否かを判定するデバイスリスト判定部と、

前記デバイスリスト判定部でリボークすべきと判断された場合には前
25 記記録媒体の再生動作を制限する制御部を有する請求の範囲第35項に記載の再生装置。

39. 前記デバイス・リボケーション・リストが、前記著作権管理サーバから更新される請求の範囲第38項に記載の再生装置。

40. 複数の再生装置と著作権管理者の認可を受けた著作権管理サーバとがネットワークを介して接続されたシステムにおける著作権管理方法
5 において、

再生装置のそれぞれは、ビデオコンテンツのデータが記録され、一連の記録媒体毎に、各記録媒体を一意に識別する媒体識別情報が記録されている記録媒体を再生し、

記録媒体の前記媒体識別情報を読み出し、読み出した前記媒体識別情報から一方向性の関数により得られる識別メッセージを機器識別情報と共に前記著作権管理サーバに送信し、
10

前記著作権管理サーバは、前記機器識別情報と前記識別メッセージとを受信し、

受信データの集合から複数の再生装置における同一の記録媒体の再生
15 の有無を検出し、

ある一定以上の台数の再生装置によって同一の前記媒体識別情報の記録媒体の再生が検出された場合には、当該記録媒体を指示する少なくとも前記媒体識別情報または前記識別メッセージを媒体リボケーション・リストに追加する更新を行う著作権管理方法。

41. 時刻情報に基づいて生成され、所定の機構で読み出された場合に著作権管理者が許可する層まで前記所定の機構を有する機器において再生動作を制限するシグネチャ・データが電子透かしとして埋め込まれているビデオコンテンツのデータが記録されている記録媒体を再生する再生方法であって、
20

再生された際に、前記記録媒体から前記シグネチャ・データを検出するシグネチャ・データ検出ステップと、
25

前記検出されたシグネチャ・データに基づいて、前記所定の機構を有する機器内に再生の制限を行う暦情報であるシグネチャ・データのリストを生成させるリスト生成ステップと、

5 前記リストに含まれている限り、前記所定の機構を有する機器において、著作権管理者が許可する暦まで前記シグネチャ・データが記録された記録媒体の再生動作を制限する再生制限ステップを有する再生方法。

4 2. 前記リスト生成ステップが、外部からの改竄が困難なタイマを有しており、前記検出されたシグネチャ・データに基づいて前記タイマを参照して前記シグネチャ・データのリストを生成する請求の範囲第 4 1
10 項に記載の再生方法。

4 3. 前記タイマが、前記所定の機構を有する機器とネットワークを介して接続する著作権管理サーバにより較正される請求の範囲第 4 2 項に記載の再生方法。

4 4. 前記リスト生成ステップが、前記検出されたシグネチャ・データ
15 に基づいて、前記所定の機構を有する機器とネットワークを介して接続する著作権管理サーバが有する外部からの改竄が困難なタイマを参照して前記シグネチャ・データのリストを生成する請求の範囲第 4 1 項に記載の再生方法。

4 5. ビデオコンテンツのデータが記録されている記録媒体を再生する
20 再生装置であって、

再生された際に、前記ビデオコンテンツのデータに電子透かしとして埋め込まれている、時刻情報に基づいて生成され、著作権管理者が許可する暦まで再生動作を制限するシグネチャ・データを検出するシグネチャ・データ検出部と、

25 前記検出されたシグネチャ・データに基づいて、再生の制限を行う暦情報であるシグネチャ・データのリストを生成させるリスト生成部と、

前記リストに含まれている限り、著作権管理者が許可する暦まで前記シグネチャ・データが記録された記録媒体の再生動作を制限する制御部とを有する再生装置。

46. 前記リスト生成部が、外部からの改竄が困難なタイマを有しており、前記検出されたシグネチャ・データに基づいて前記タイマを参照して前記シグネチャ・データのリストを生成する請求の範囲第45項に記載の再生装置。

47. 前記タイマが、ネットワークを介して接続する著作権管理サーバにより較正される請求の範囲第46項に記載の再生装置。

- 10 48. 前記リスト生成部が、前記検出されたシグネチャ・データに基づいて、ネットワークを介して接続する著作権管理サーバが有する外部からの改竄が困難なタイマを参照して前記シグネチャ・データのリストを生成する請求の範囲第45項に記載の再生装置。

- 15 49. 複数の再生装置と著作権管理者の認可を受けた著作権管理サーバとがネットワークを介して接続された著作権管理システムにおける著作権管理方法において、

- 時刻情報に基づいて生成され、所定の機構で読み出される場合に著作権管理者が許可する暦まで前記所定の機構を有する機器において再生動作を制限するシグネチャ・データを、ビデオコンテンツに対して電子透かし情報として埋め込み、

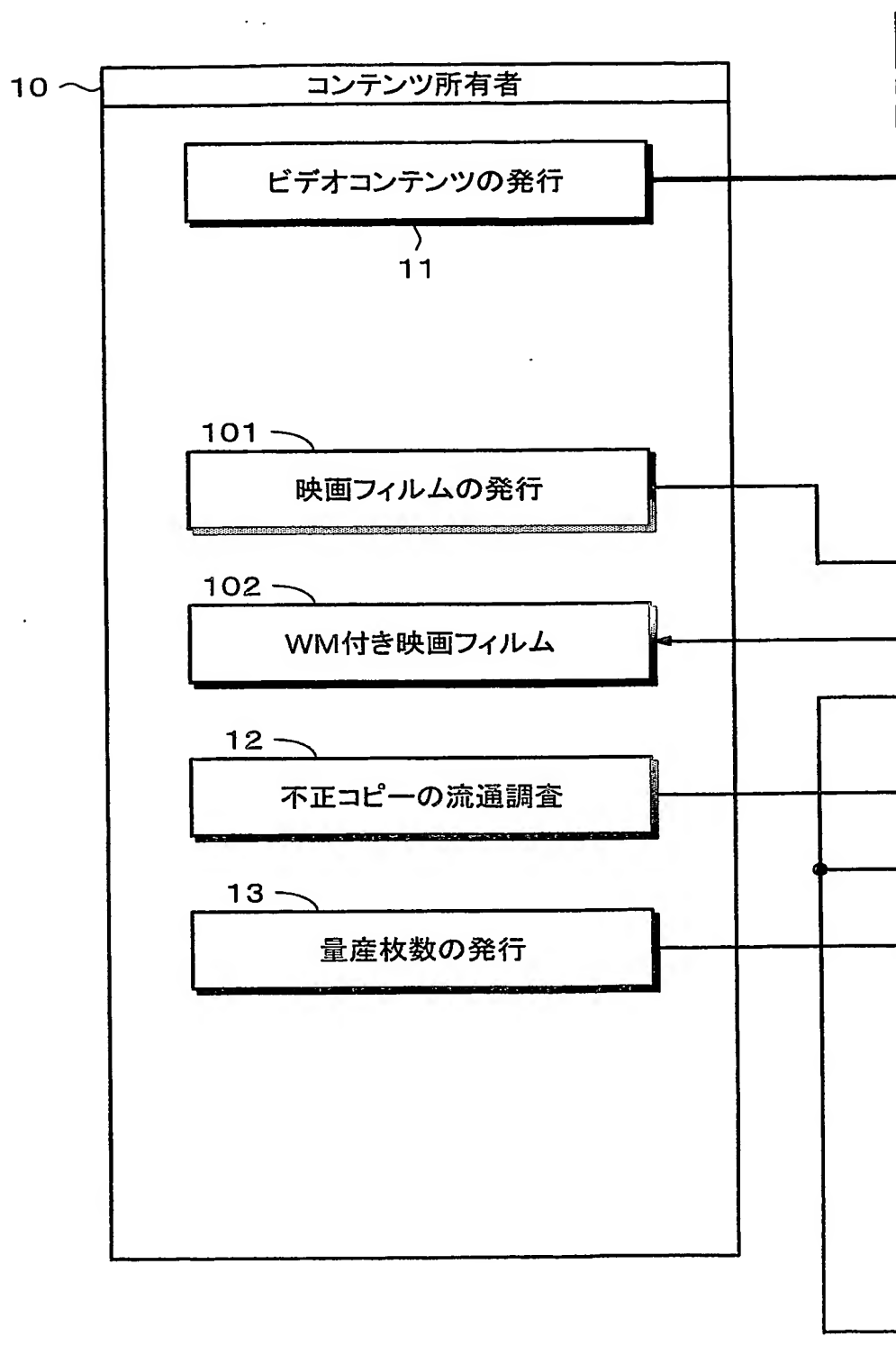
前記機器のそれぞれは、ビデオコンテンツを再生する際に、前記シグネチャ・データを検出し、検出された前記シグネチャ・データに基づいて、再生の制限を行う暦情報であるシグネチャ・データのリストを生成し、

- 25 前記リストに含まれている限り、前記機器において、著作権管理者が許可する暦まで前記シグネチャ・データが記録された記録媒体の再生動

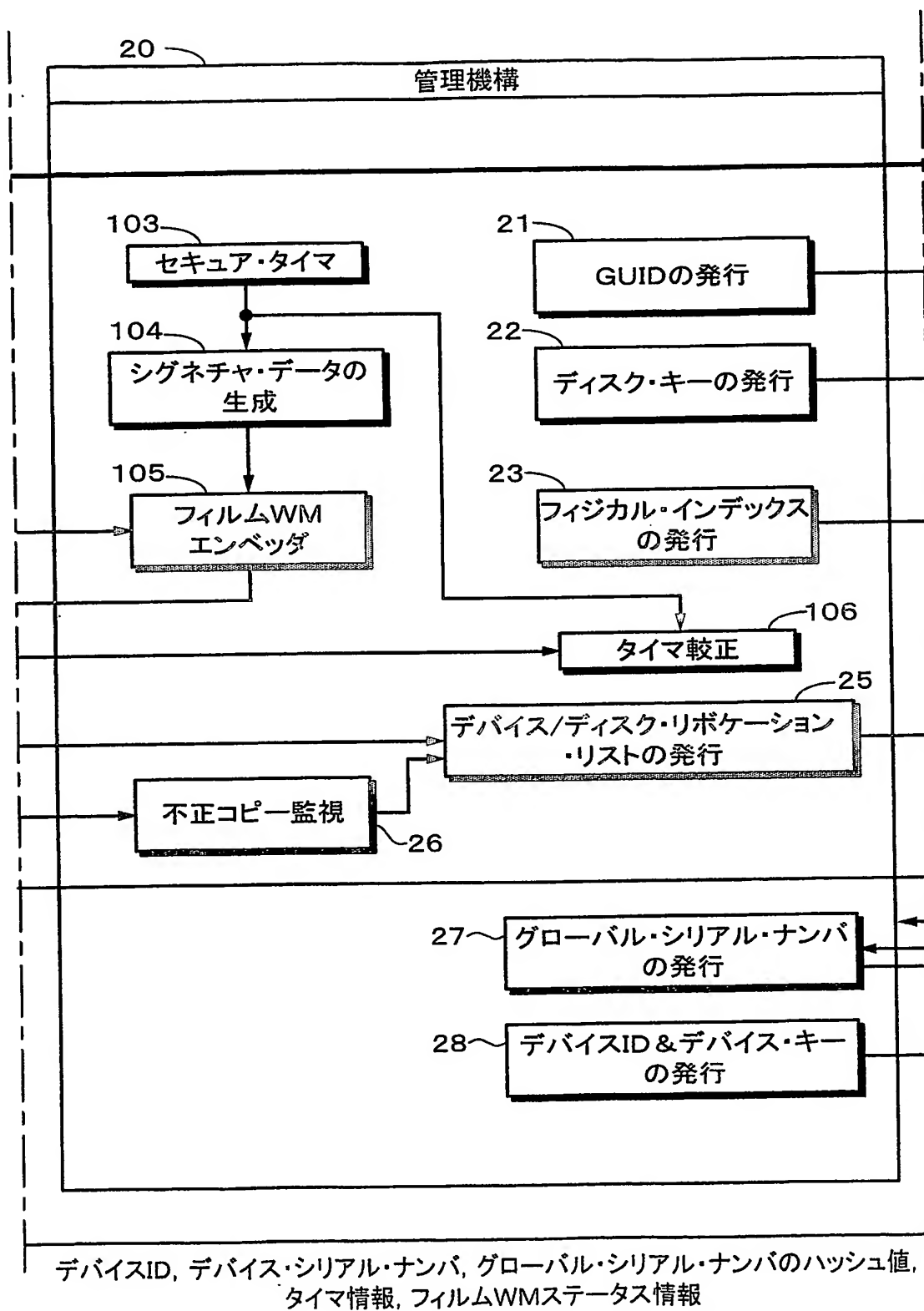
作を制限する著作権管理方法。

50. 前記機器の持つ前記シグネチャ・リストが前記著作権管理サーバによって更新される請求の範囲第49項に記載の著作権管理方法。

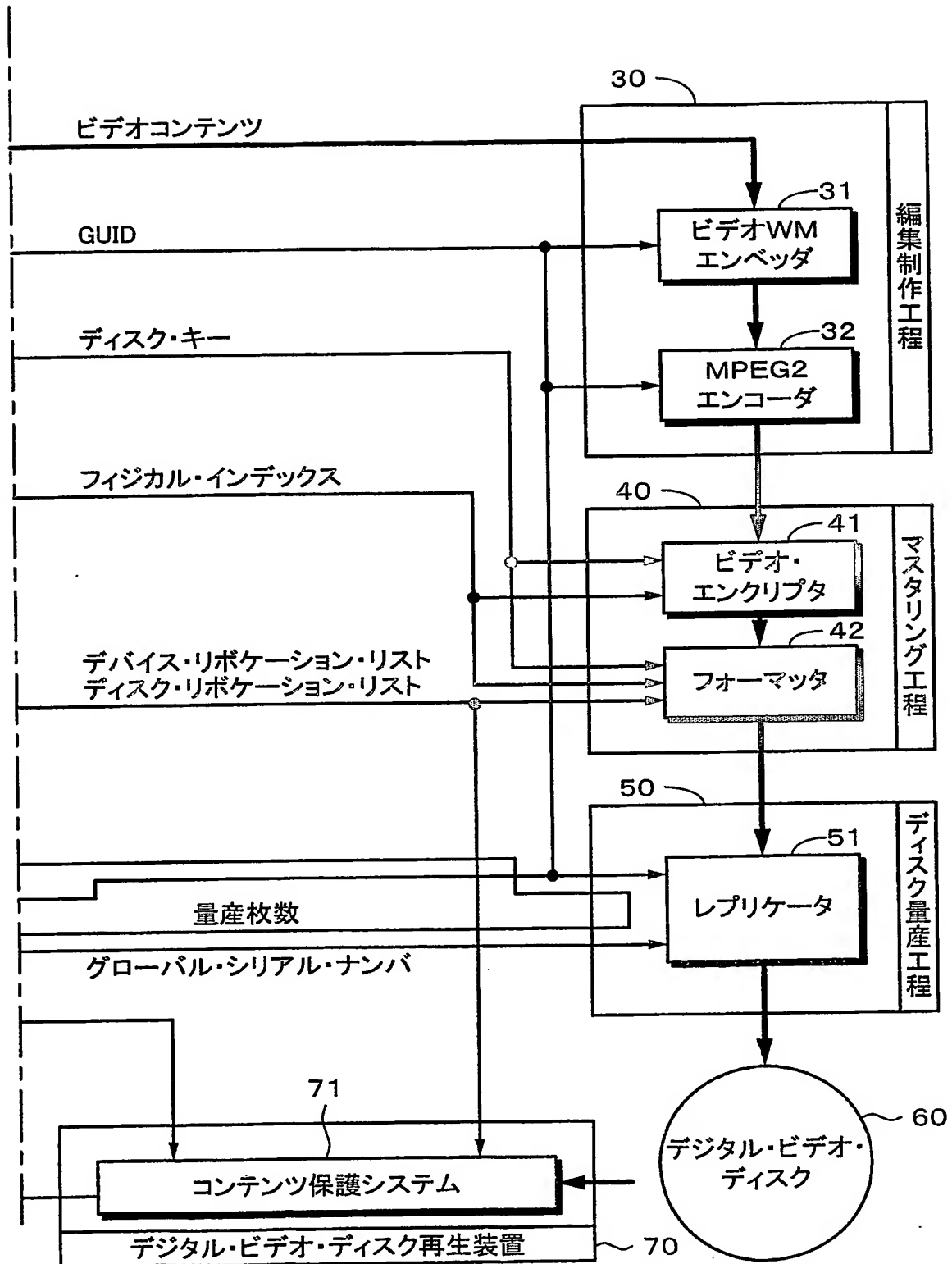
第1図



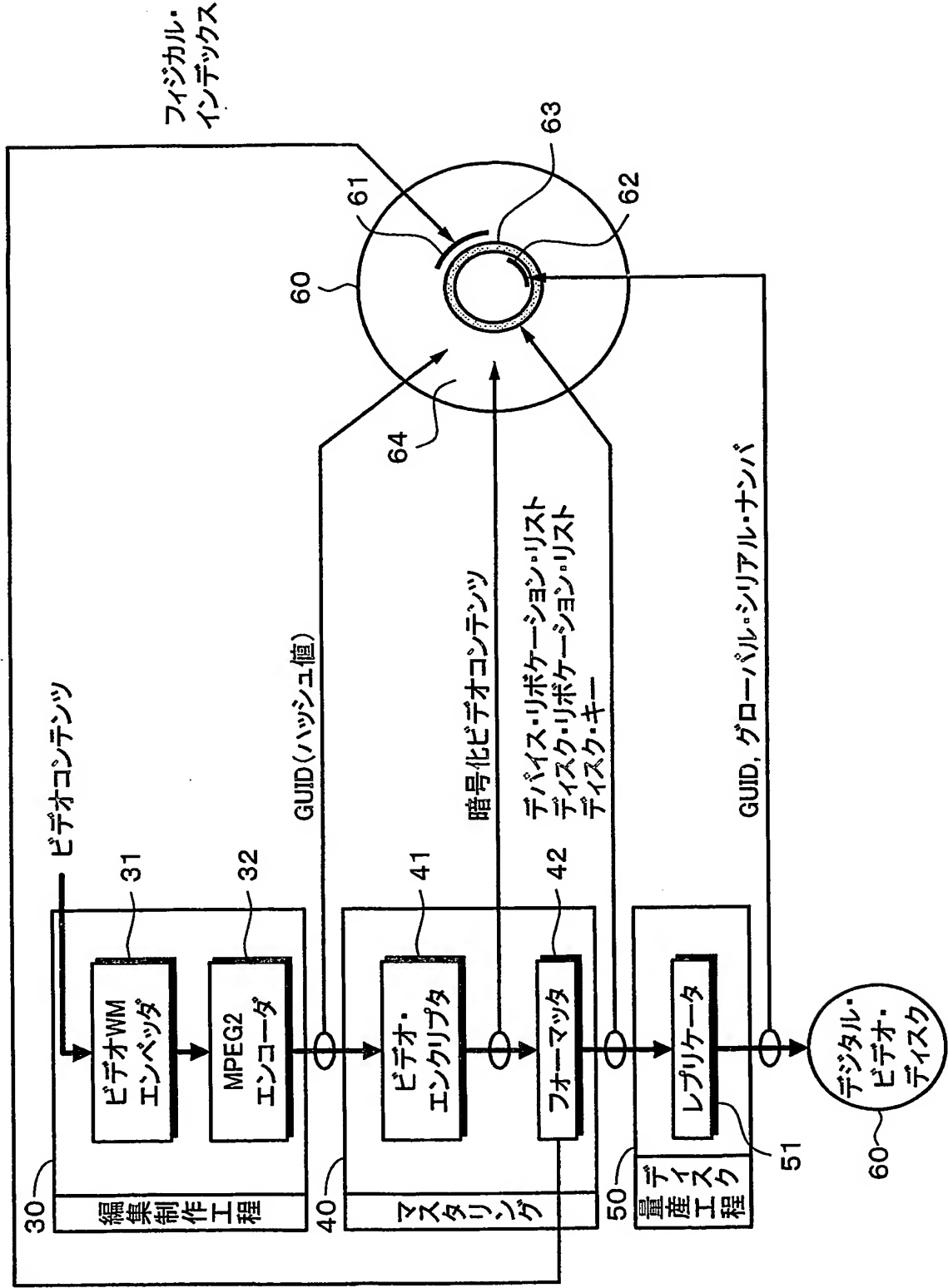
第2図



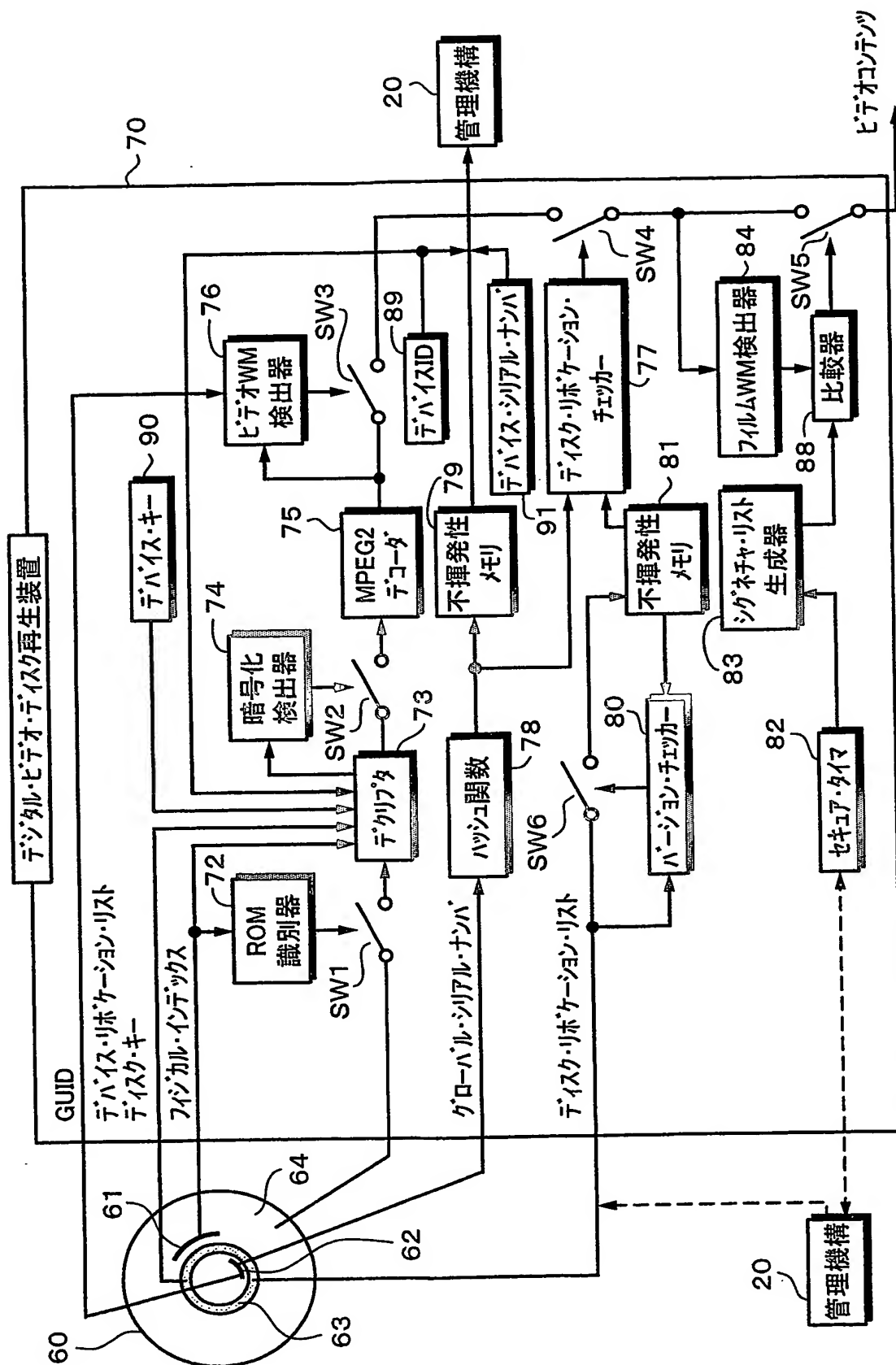
第3図



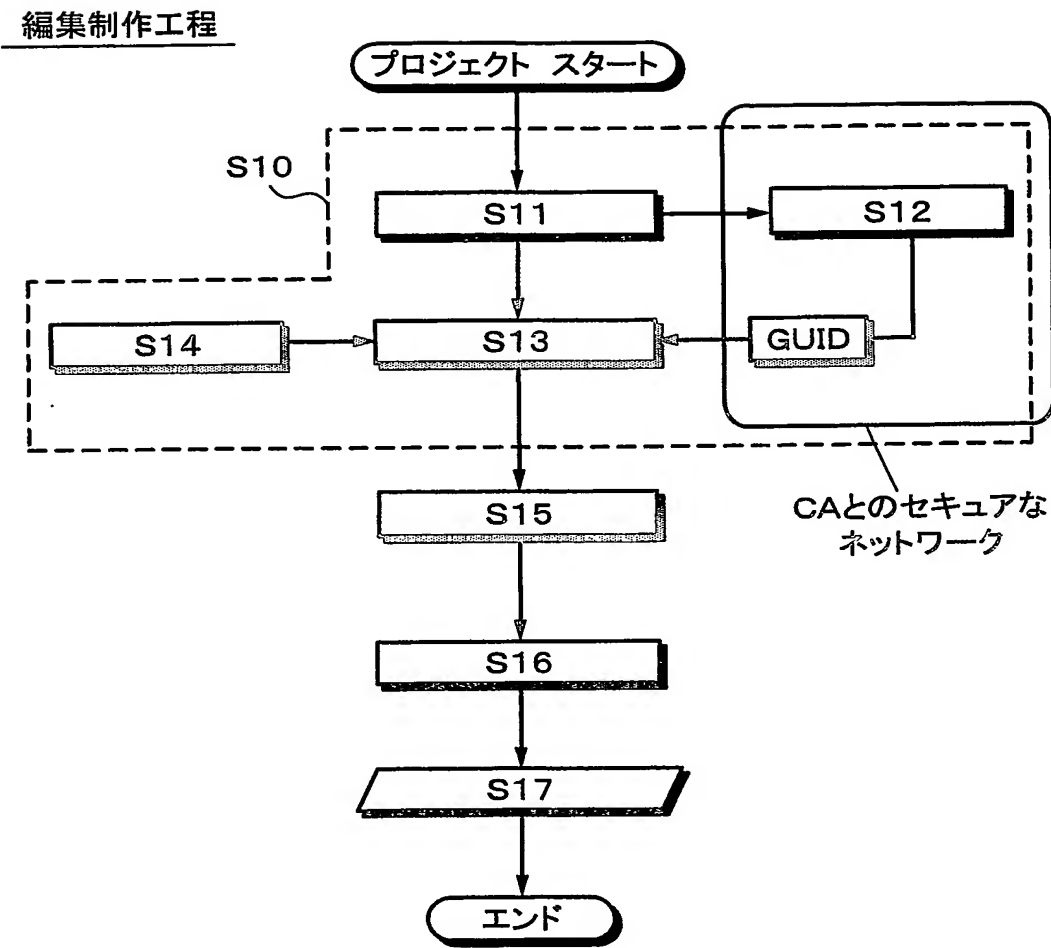
第4図



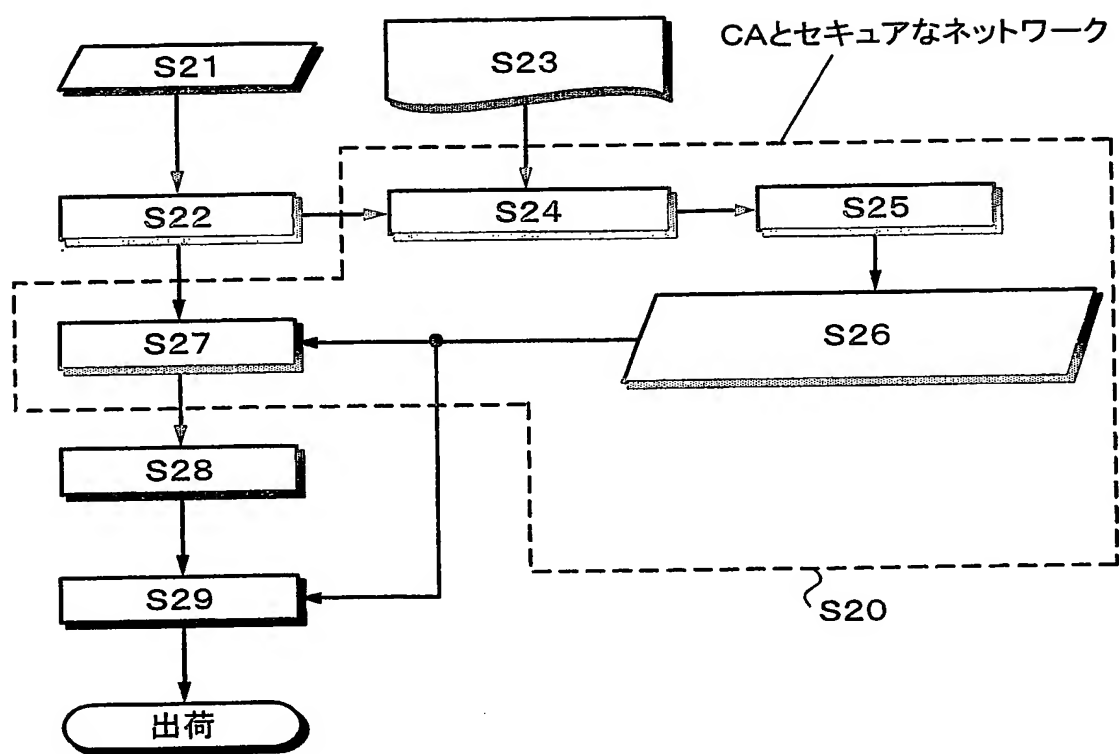
無



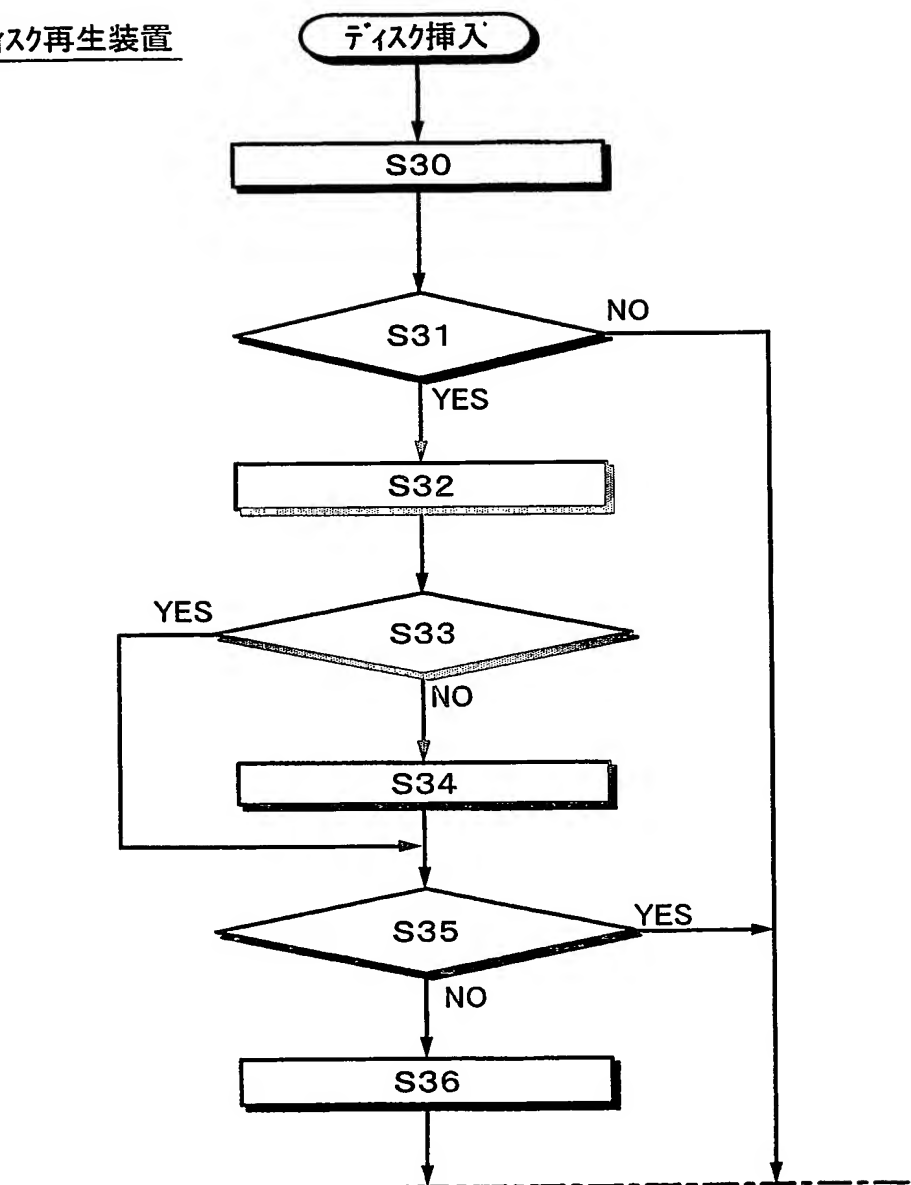
第 6 図



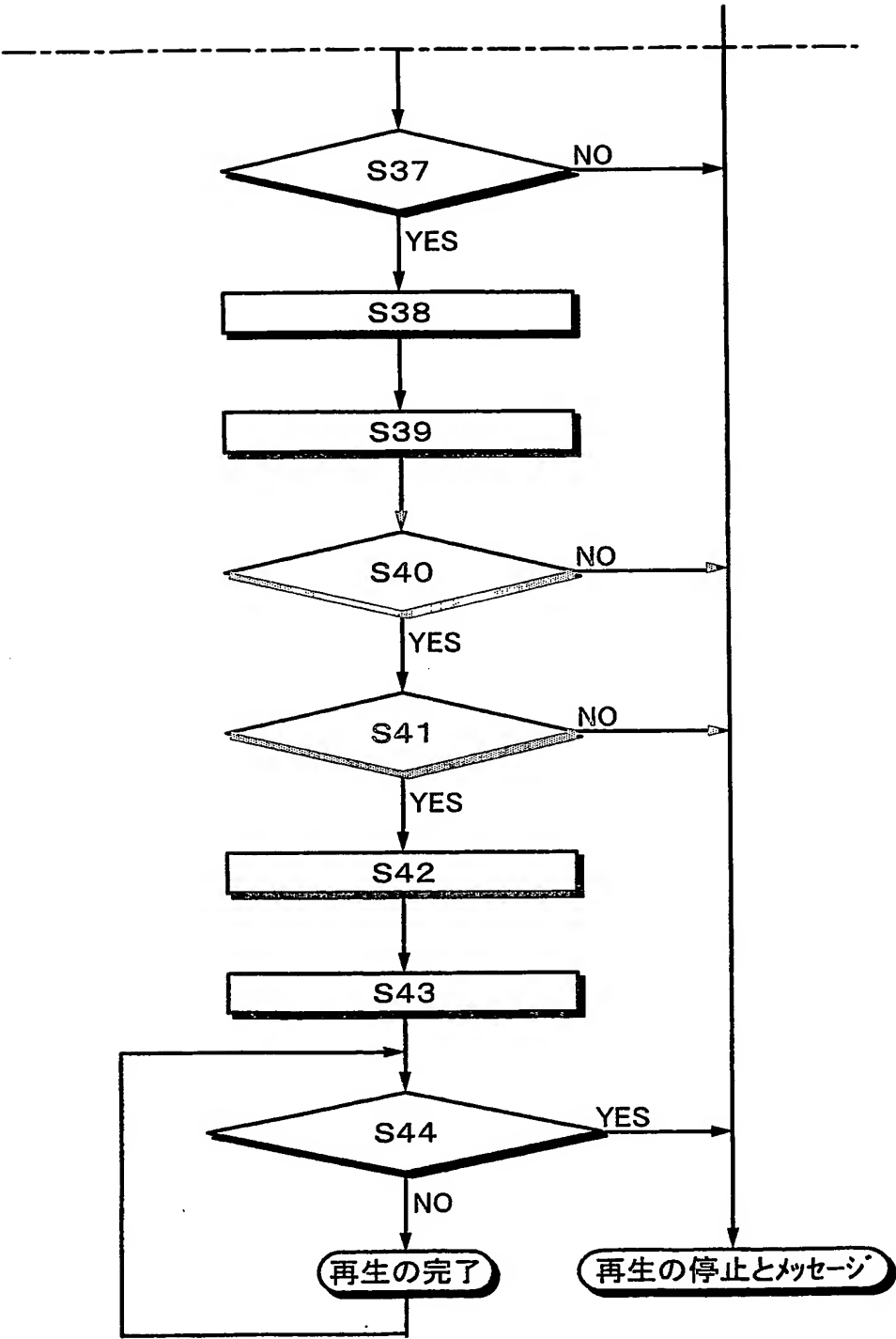
第7図

ディスク製造工程

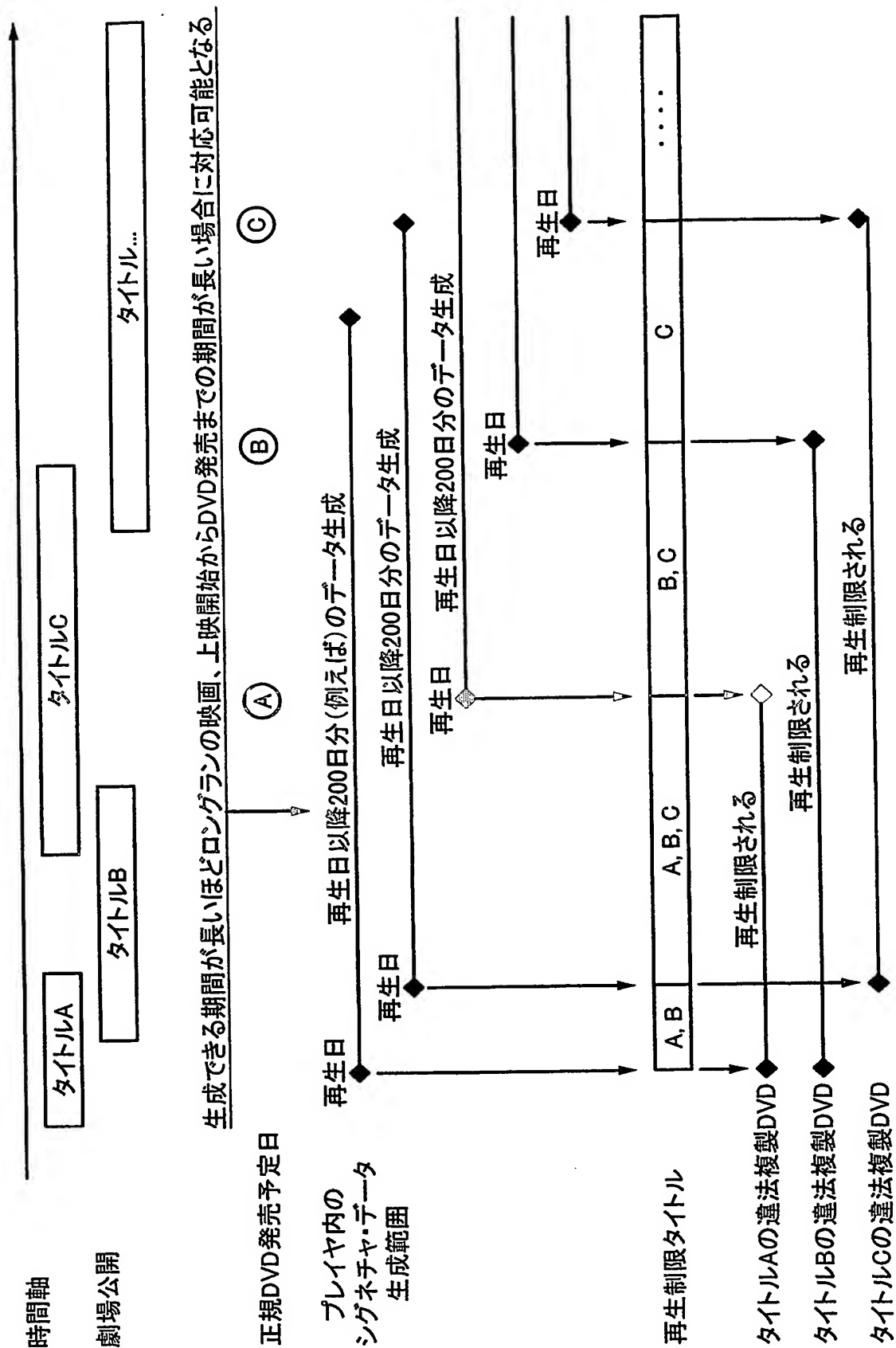
第 8 図

ディスク再生装置

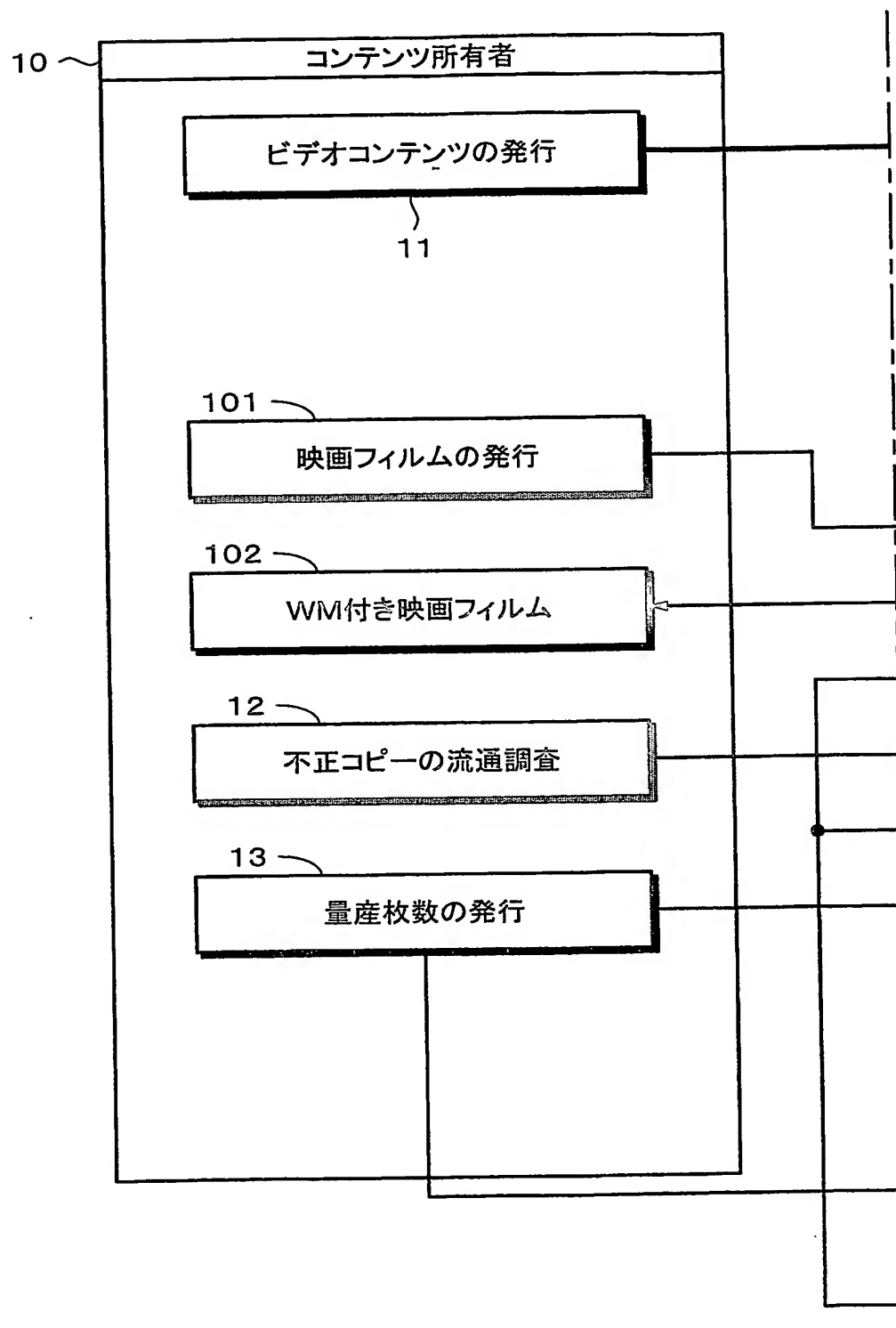
第 9 図



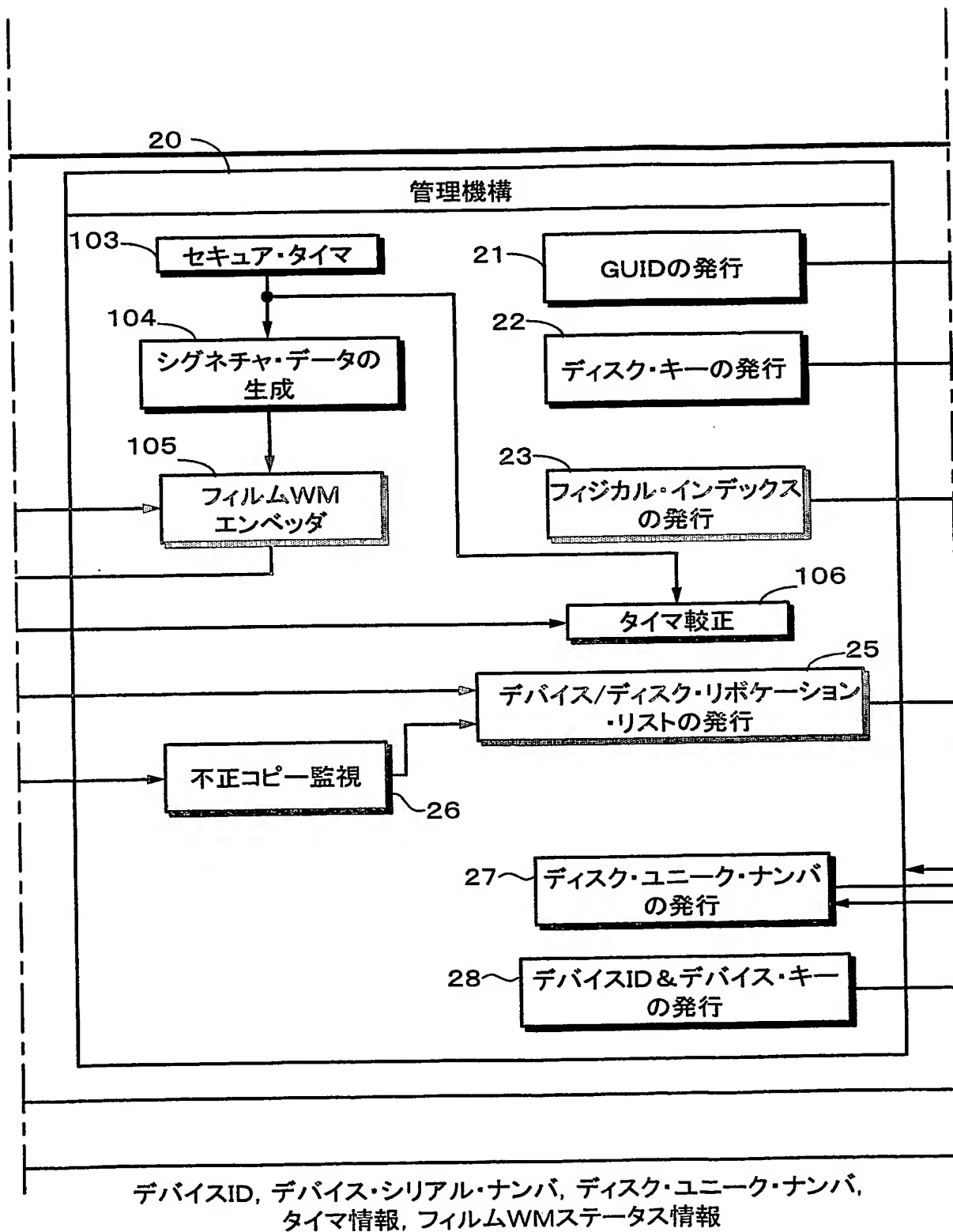
第 10 圖



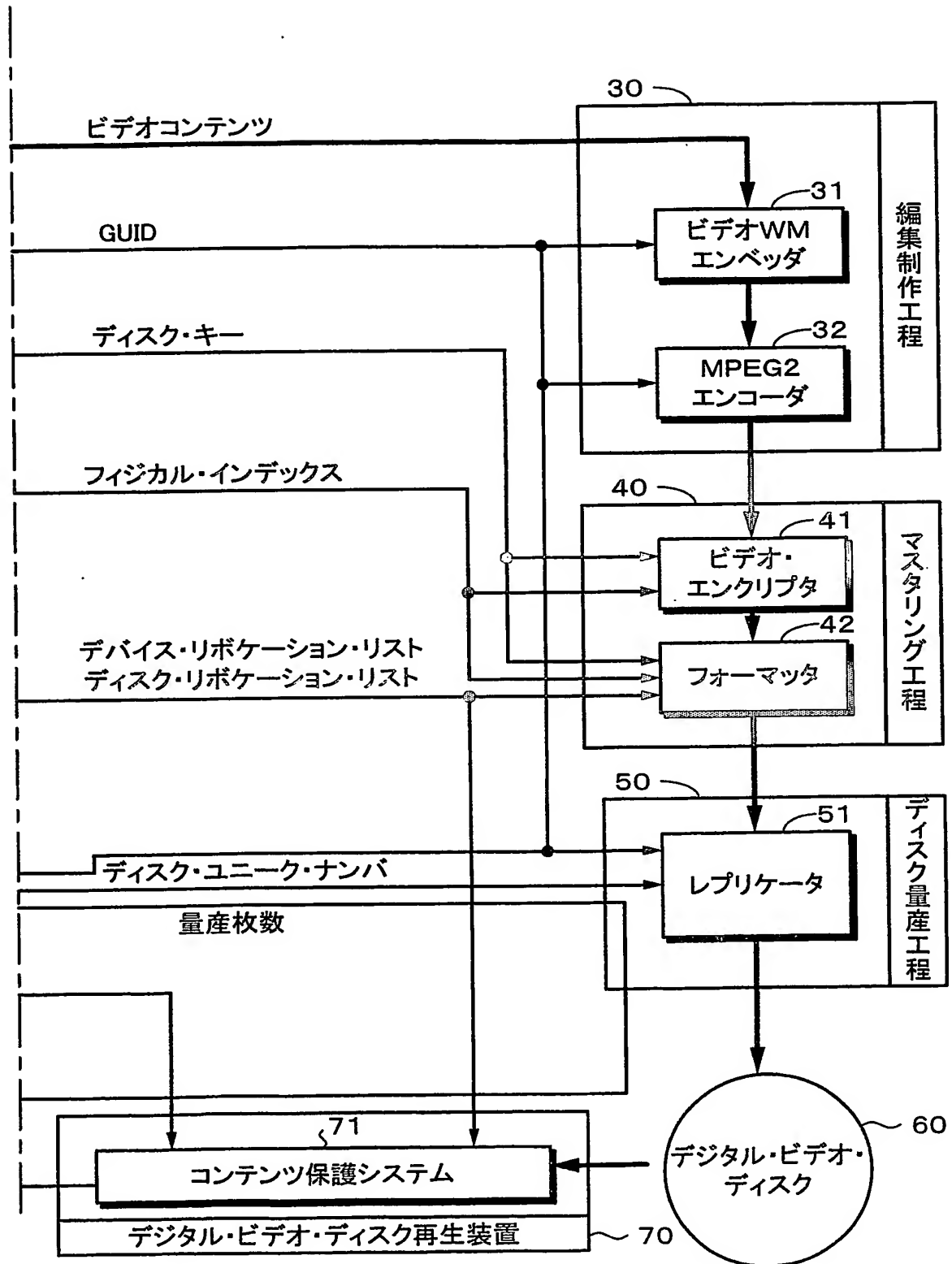
第 1 1 図



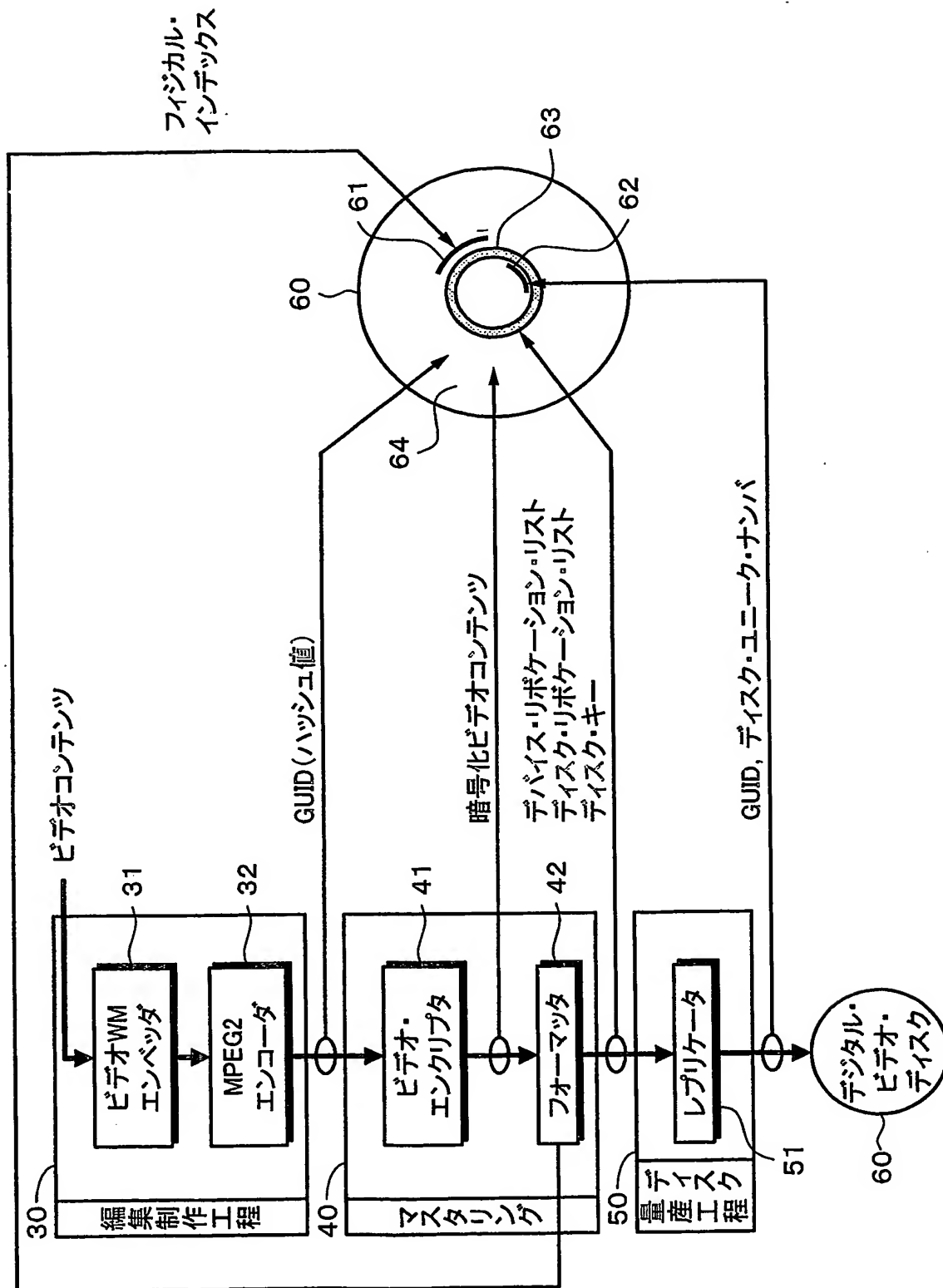
第12図



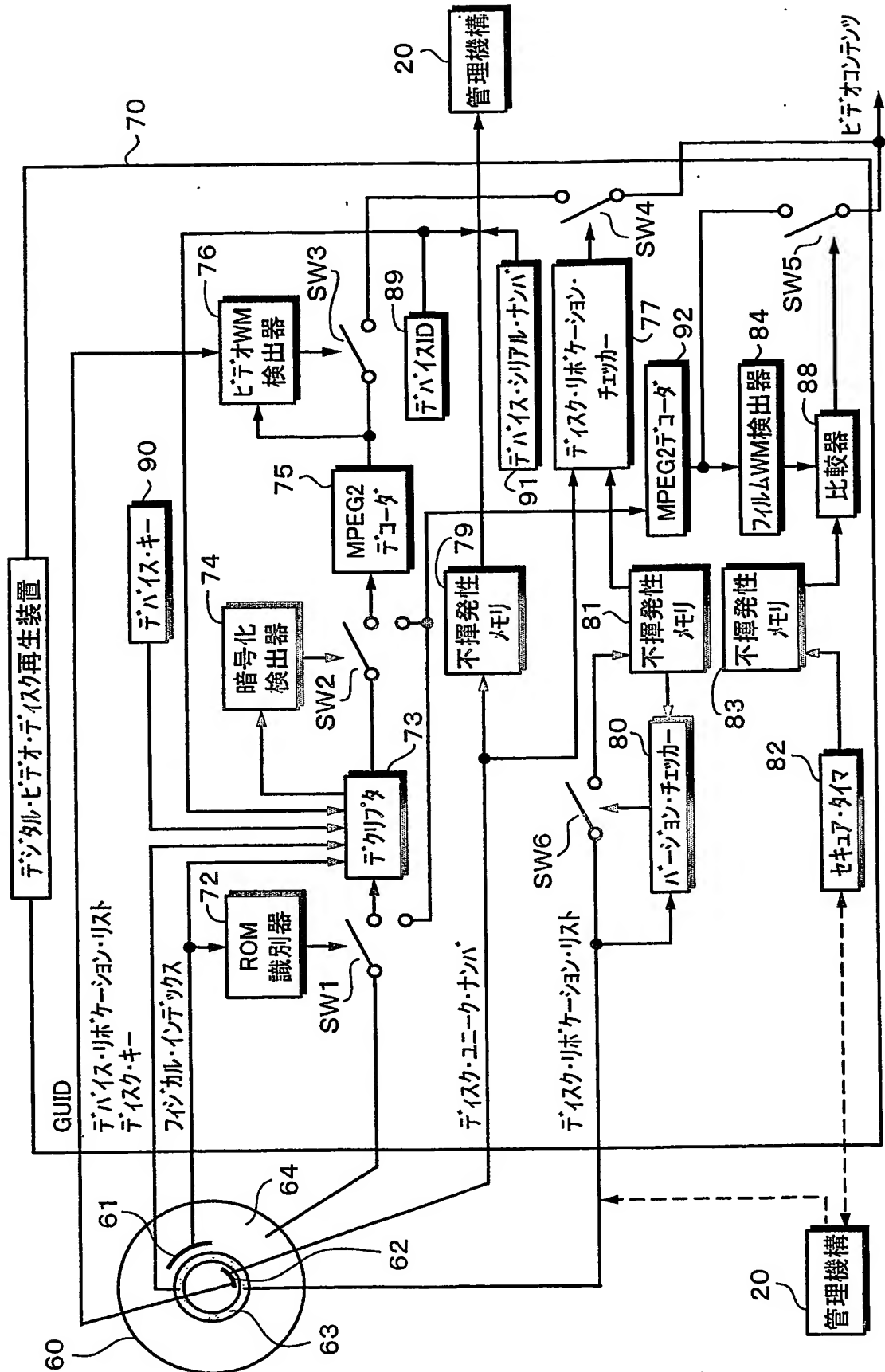
第13図



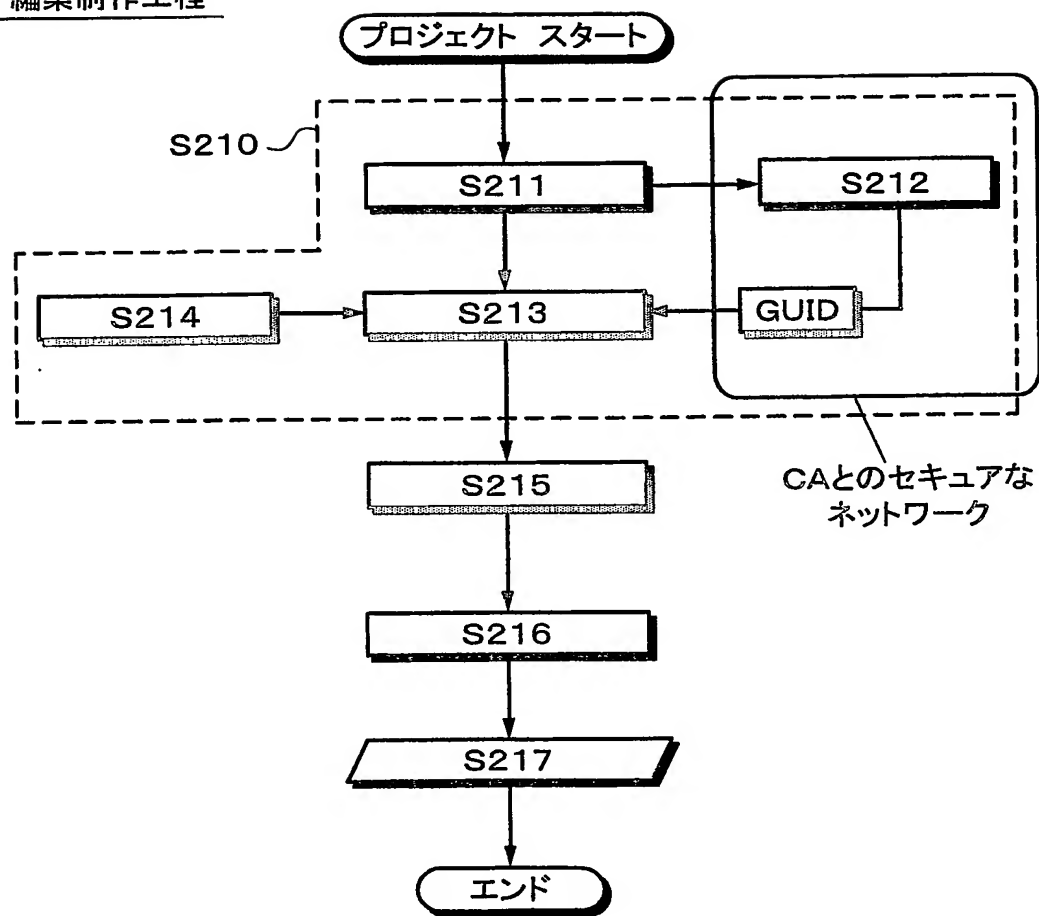
第14図



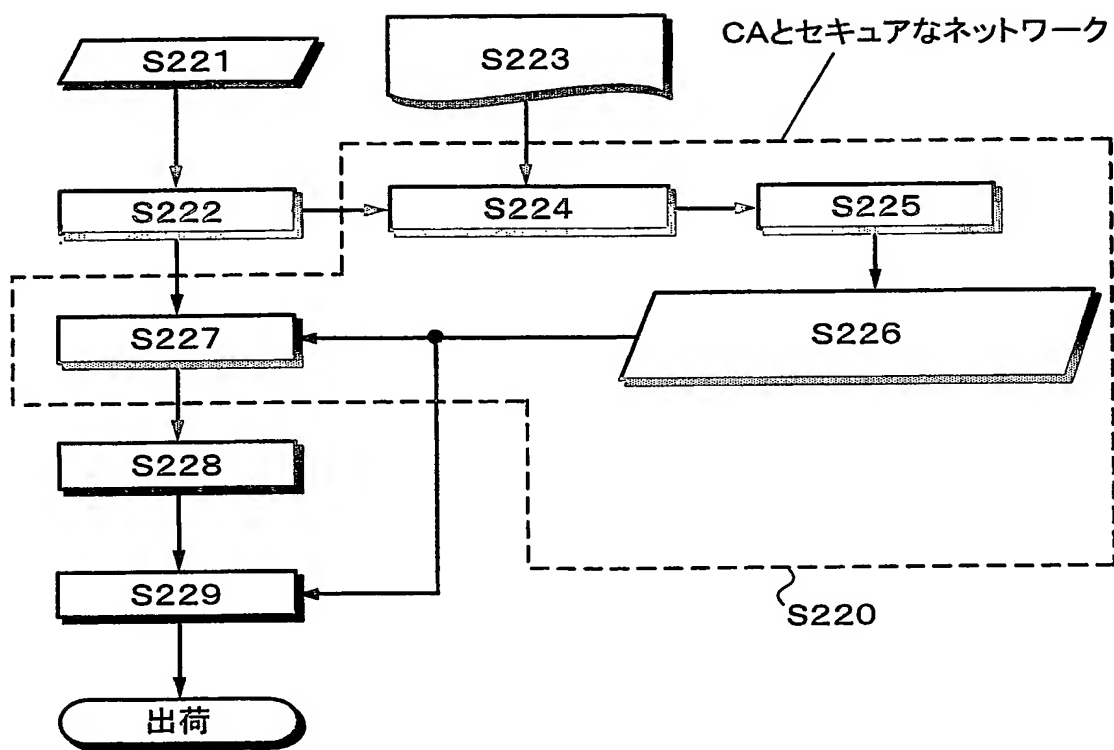
第15図



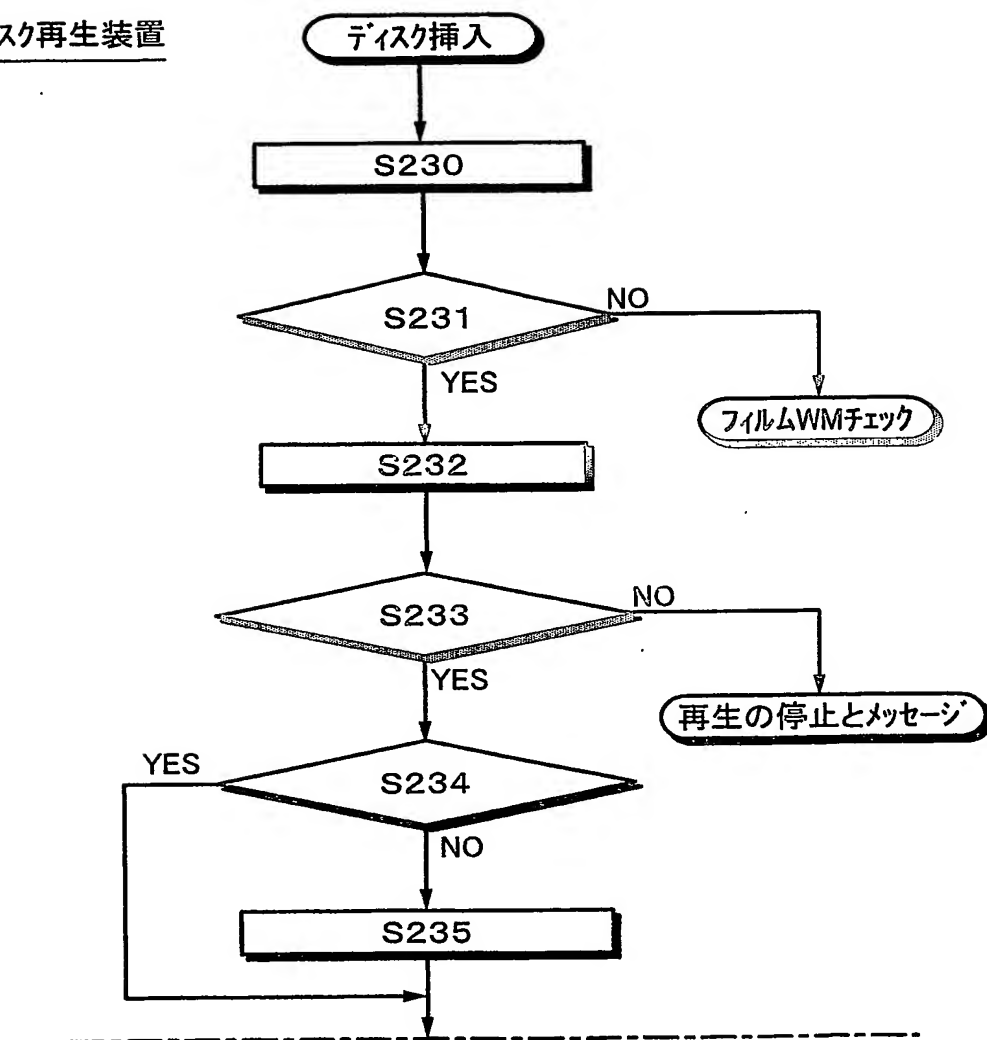
第 16 図

編集制作工程

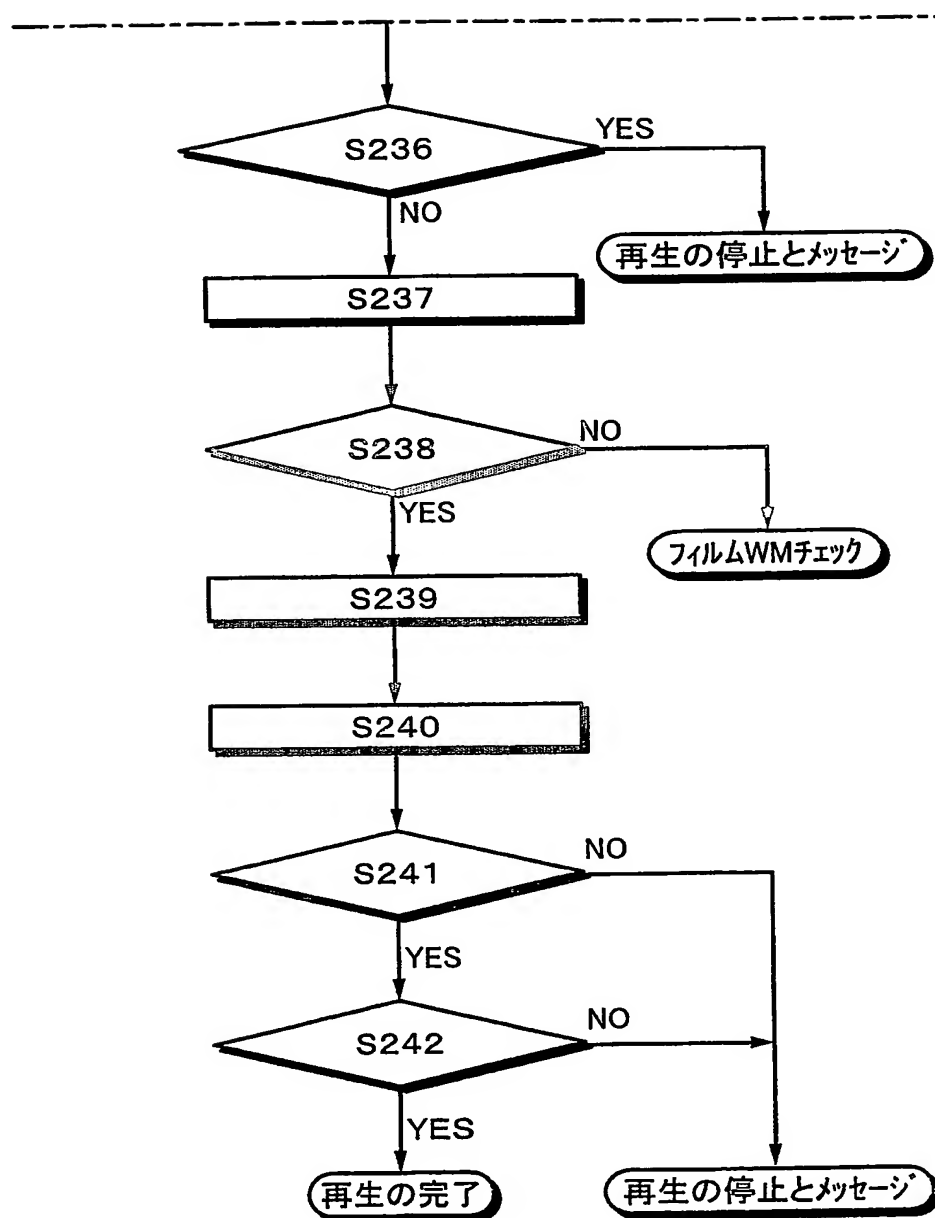
第 17 図

ディスク製造工程

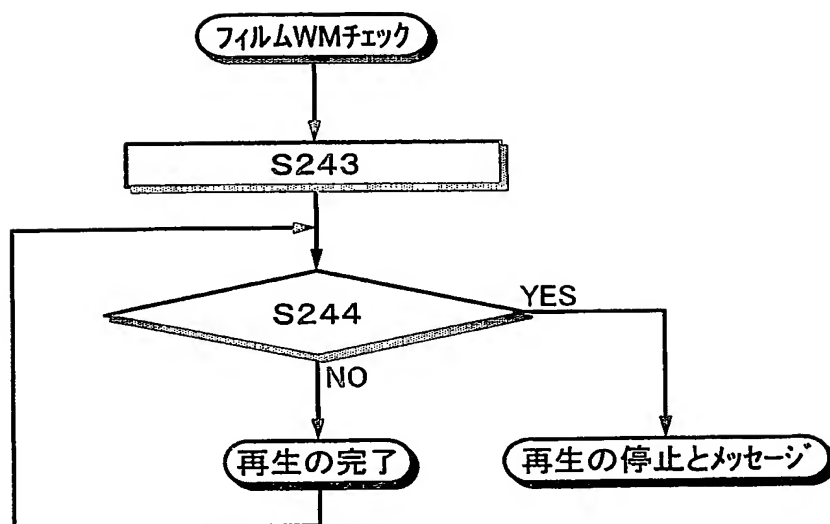
第18図

ディスク再生装置

第 1 9 図



第 2 0 図



符号の説明

1 0	コンテンツ所有者
2 0	管理機構
3 0	編集制作工程
4 0	マスタリング工程
5 0	ディスク量産工程
6 0	デジタル・ビデオ・ディスク
7 0	デジタル・ビデオ・ディスク再生装置
6 1	フィジカル・ウォーターマーク
6 2	B C A
6 3	リードインエリア
6 4	データエリア
7 2	R O M 識別器
7 4	暗号化検出器
7 6	ビデオ電子透かし検出器
7 7	ディスク・リボケーション・チェッカー
7 9, 8 1	不揮発性メモリ
8 0	バージョン・チェッカー
8 2	セキュア・タイマ
8 3	シグネチャ・リスト生成器
8 4	フィルム電子透かし検出器
8 8	比較器
S 1 1	C A への G U I D の要求
S 1 2	G U I D の発行
S 1 3	ビデオWMの埋め込み

- S 1 4 ビデオWMの提供
- S 1 5 オーディオ等のエンコード
- S 1 6 マルチプレックスおよびGUIDの挿入
- S 1 7 マスタフォーマットへのディスクイメージの書き込み
- S 2 1 ディスクイメージの受け取り
- S 2 2 GUIDの抽出
- S 2 3 枚数の発注 (n = 量産枚数)
- S 2 4 GUIDの送出とシリアル番号の要求
- S 2 5 管理機構
- S 2 6 ディスク製造の許諾 (1. ディスク・キー、フィジカル・インデックスの転送、2. シリアル番号、デバイス・リボケーション・リスト、ディスク・リボケーション・リストの転送)
- S 2 7 ディスク・マスターの作成
- S 2 8 リプリケーション
- S 2 9 ユニークIDによるポストマーク (GUID、グローバル・シリアル・ナンバ)
- S 3 0 フィジカル・インデックスの読み出し
- S 3 1 検出されたか？
- S 3 2 BCAの読み出し (GUID、グローバル・シリアル・ナンバ)
- S 3 3 同一のシリアル・ナンバが蓄積されているか？
- S 3 4 シリアル・ナンバの蓄積
- S 3 5 シリアル・ナンバがリボークされているか？
- S 3 6 リードインエリアの読み出し (デバイス・リボケーション・リスト、ディスク・リボケーション・リスト、

- ディスク・キー)
- S 3 7 暗号化?
 - S 3 8 ディスク・リポケーション・リストの更新
 - S 3 9 再生開始
 - S 4 0 ビデオWMが存在?
 - S 4 1 WM=GUIDのハッシュ値?
 - S 4 2 再生継続
 - S 4 3 シグネチャ・リストの生成とフィルムWMステータスとの比較
 - S 4 4 ステータスとシグネチャ・リストが一致?
 - S 2 1 1 CAへのGUIDの要求
 - S 2 1 2 GUIDの発行
 - S 2 1 3 ビデオWMの埋め込み
 - S 2 1 4 ビデオWMの提供
 - S 2 1 5 オーディオ等のエンコード
 - S 2 1 6 マルチプレックスおよびGUIDの挿入
 - S 2 1 7 マスタフォーマットへのディスクイメージの書き込み
 - S 2 2 1 ディスクイメージの受け取り
 - S 2 2 2 GUIDの抽出
 - S 2 2 3 枚数の発注 (n = 量産枚数)
 - S 2 2 4 GUIDの送出とディスク・ユニーク番号の要求
 - S 2 2 5 管理機構
 - S 2 2 6 ディスク製造の許諾 (1. ディスク・キー、フィジカル・インデックスの転送、2. ユニーク番号、デバイス・リポケーション・リスト、ディスク・リポケーション・リストの転送)

- S 2 2 7 ディスク・マスターの作成
- S 2 2 8 リプリケーション
- S 2 2 9 ユニーク I D によるポストマーク (G U I D、ディスク・ユニーク・ナンバ)
- S 2 3 0 フィジカル・インデックスの読み出し
- S 2 3 1 検出されたか？
- S 2 3 2 B C A の読み出し (G U I D、ディスク・ユニーク・ナンバ)
- S 2 3 3 ディスク・ユニーク・ナンバの確認？
- S 2 3 4 同一のユニーク・ナンバが蓄積されているか？
- S 2 3 5 ユニーク・ナンバの蓄積
- S 2 3 6 ユニーク・ナンバがリボークされているか？
- S 2 3 7 リードインエリアの読み出し (デバイス・リボケーション・リスト、ディスク・リボケーション・リスト、ディスク・キー)
- S 2 3 8 暗号化？
- S 2 3 9 ディスク・リボケーション・リストの更新
- S 2 4 0 再生開始
- S 2 4 1 ビデオWMが存在？
- S 2 4 2 WM = G U I D のハッシュ値？
- S 2 4 3 シグネチャ・リストの生成とフィルムWMステータスとの比較
- S 2 4 4 ステータスとシグネチャ・リストが一致？

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/003077

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G11B20/10, G11B20/12, G11B7/005, H04N5/91, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G11B20/10-20/16, H04N5/91-5/92, G10K15/02, G06F3/06,
G06F12/14, G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-73017 A (Victor Company Of Japan, Ltd.), 12 March, 2002 (12.03.02), Column 2, lines 12 to 40; column 9, line 12 to column 10, line 8; Figs. 1, 24 to 27 & US 2002/10826 A1	1-7, 41-50
Y	JP 11-73725 A (Sony Corp.), 16 March, 1999 (16.03.99), Column 33, line 35 to column 35, line 20; Figs. 1, 6, 8, 9 & US 6282654 B1	1-7, 40-50

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
25 May, 2004 (25.05.04)Date of mailing of the international search report
08 June, 2004 (08.06.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/003077

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-251395 A (Matsushita Electric Industrial Co., Ltd.), 14 September, 2000 (14.09.00), Column 10, line 43 to column 14, line 37; Figs. 1 to 7 & EP 1158514 A1	1-50
Y	JP 2000-148014 A (NTT Data Corp.), 26 May, 2000 (26.05.00), Column 3, line 7 to column 4, line 45; Fig. 1 (Family: none)	1-39
Y	JP 2000-155834 A (Canon Inc.), 06 June, 2000 (06.06.00), Column 8, line 49 to column 9, line 27 (Family: none)	1-39
Y	JP 2002-135243 A (Sony Corp.), 10 May, 2002 (10.05.02), Column 19, line 43 to column 21, line 20; column 27, line 29 to column 30, line 50; column 56, line 25 to column 58, line 2; Figs. 2, 4, 9, 16 to 18, 47 & EP 1235380 A1 & US 2002/184259 A1	8-39
Y	WO 2000/046804 A1 (Sony Corp.), 10 August, 2000 (10.08.00), Page 9, line 15 to page 17, line 17; Figs. 1 to 5 & EP 1069567 A1	8-39
Y	JP 2001-211151 A (Sony Corp.), 03 August, 2001 (03.08.01), Column 114, line 11 to column 118, line 46; Figs. 86 to 88 & EP 1195734 A1 & EP 1267515 A1	8-39
Y	JP 2000-357126 A (Toshiba Corp.), 26 December, 2000 (26.12.00), Full text; Figs. 1 to 6 & EP 1067447 A2	8-39
Y	JP 2001-175603 A (Kansai TLO Kabushiki Kaisha), 29 June, 2001 (29.06.01), Column 6, line 36 to column 11, line 23; Figs. 1 to 3 (Family: none)	40
Y	JP 11-232775 A (Matsushita Electric Industrial Co., Ltd.), 27 August, 1999 (27.08.99), Column 10, line 32 to column 13, line 36; Figs. 4 to 6 (Family: none)	40

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/003077

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-74836 A (Canon Inc.), 15 March, 2002 (15.03.02), Column 8, line 11 to column 10, line 40; Figs. 1 to 5 (Family: none)	41-50

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/JP2004/003077

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-7 relate to a technical feature for comparing, upon reproduction, title information embedded as an electronic watermark in the video content to the title information recorded in a recording area different from the area where the content data is recorded and judging whether the validity is guaranteed.

The inventions of claims 8-39 relate to a technical feature for judging whether the medium identification information on the recording medium is contained in the revocation list.

(Continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

Continuation of Box No. III of continuation of first sheet (2)

The invention of claim 40 relates to a technical feature for detecting presence/absence of reproduction of the same recording medium in a plurality of reproduction devices by using the medium identification information on the recording medium.

The inventions of claims 41-50 relate to a technical feature for limiting the reproduction operation until the date allowed by the copyright manager according to the signature data generated according to the time information and embedded in the video content.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G11B20/10, G11B20/12, G11B7/005,
H04N5/91, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G11B20/10-20/16, H04N5/91-5/92, G10K15/02
G06F3/06, G06F12/14, G09C1/00, H04L9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2004年
日本国登録実用新案公報 1994-2004年
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-73017 A (日本ビクター株式会社) 2002. 03. 12, 第2欄第12行~第40行, 第9欄第12行~第10欄第8行, 第1, 24-27図 & US 2002/10826 A1	1-7, 41-50
Y	JP 11-73725 A (ソニー株式会社) 1999. 03. 16, 第33欄第35行~第35欄第20行, 第1, 6, 8, 9図 & US 6282654 B1	1-7, 40-50

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

25. 05. 2004

国際調査報告の発送日

08. 6. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

早川 卓哉

5Q

9295

電話番号 03-3581-1101 内線 3590

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2000-251395 A (松下電器産業株式会社) 2000. 09. 14, 第10欄第43行~第14欄第37行, 第1-7図 & EP 1158514 A1	1-50
Y	JP 2000-148014 A (株式会社エヌ・ティ・ティ・ データ) 2000. 05. 26, 第3欄第7行~第4欄第45行, 第1図 (ファミリーなし)	1-39
Y	JP 2000-155834 A (キヤノン株式会社) 2000. 06. 06, 第8欄第49行~第9欄第27行 (ファミリーなし)	1-39
Y	JP 2002-135243 A (ソニー株式会社) 2002. 05. 10, 第19欄第43行~第21欄第20行, 第27欄第29行~第30欄第50行, 第56欄第25行~ 第58欄第2行, 第2, 4, 9, 16-18, 47図 & EP 1235380 A1 & US 2002/184259 A1	8-39
Y	WO 2000/046804 A1 (ソニー株式会社) 2000. 08. 10, 第9頁第15行~第17頁第17行, 第1-5図 & EP 1069567 A1	8-39
Y	JP 2001-211151 A (ソニー株式会社) 2001. 08. 03, 第114欄第11行~第118欄第46 行, 第86-88図 & EP 1195734 A1 & EP 1267515 A1	8-39
Y	JP 2000-357126 A (株式会社東芝) 2000. 12. 26, 全文, 第1-6図 & EP 1067447 A2	8-39
Y	JP 2001-175603 A (関西ティー・エル・オー株式 会社) 2001. 06. 29, 第6欄第36行~第11欄第23 行, 第1-3図 (ファミリーなし)	40
Y	JP 11-232775 A (松下電器産業株式会社) 1999. 08. 27, 第10欄第32行~第13欄第36行, 第4-6図 (ファミリーなし)	40
Y	JP 2002-74836 A (キヤノン株式会社) 2002. 03. 15, 第8欄第11行~第10欄第40行, 第1-5図 (ファミリーなし)	41-50

第II欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第III欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-7に係る発明は、電子透かしとしてビデオコンテンツに埋め込まれたタイトル情報と、該コンテンツのデータが記録されている領域と異なる記録領域に記録されたタイトル情報を再生時に比較し、真正性が保証されているかどうか判定する技術に関するものである。

請求の範囲8-39に係る発明は、記録媒体の媒体識別情報が媒体リボケーション・リストに含まれているかどうかを判定する技術に関するものである。

請求の範囲40に係る発明は、複数の再生装置における同一の記録媒体の再生の有無を該記録媒体の媒体識別情報を用いて検出する技術に関するものである。

請求の範囲41-50に係る発明は、時刻情報に基づいて生成され、ビデオコンテンツに埋め込まれたシグナチャ・データに基づいて著作権管理者が許可する層まで再生動作を制限する技術に関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.